United States of America

Congressional Record

PROCEEDINGS AND DEBATES OF THE 114th CONGRESS, FIRST SESSION

Vol. 161 WASHINGTON, TUESDAY, AUGUST 4, 2015 No. 125

Senate

The Senate met at 10 a.m. and was called to order by the President pro tempore (Mr. HATCH).

PRAYER

The Chaplain, Dr. Barry C. Black, offered the following prayer:

Let us pray.

Eternal God, our King, let the Earth rejoice and righteousness and justice strengthen the land we love. Lord, we live in a fugitive earthly scene, but it is permeated by Your eternal presence. Remind us that transiency will not have the last word in our universe. We are grateful that life's changefulness is underlain and penetrated by Your unchanging purposes.

Guide our Senators. In these days of upheaval, show them how to find the permanent amid the impermanent, the durable amid the fragile, and the truth amid the falsehood.

Thank You for continuing to be the rock of our salvation, sustaining us in the best and worst of times.

We pray in Your strong Name. Amen.

PLEDGE OF ALLEGIANCE

The President pro tempore led the Pledge of Allegiance, as follows:

I pledge allegiance to the Flag of the United States of America, and to the Republic for which it stands, one nation under God, indivisible, with liberty and justice for all.

RECOGNITION OF THE MAJORITY LEADER

The PRESIDING OFFICER (Mr. COTTON). The majority leader is recognized.

CYBER SECURITY

Mr. MCCONNELL. Mr. President, I recently shared an AP news story with my colleagues, and I think it is worth sharing again.

Here is the headline: ''Federal Agencies Are Wide Open to Hackers, Cyberspies.''

I will read just a little bit of what it says.

The federal government, which holds secrets and sensitive information ranging from nuclear blueprints to the tax returns of hundreds of millions of Americans, has for years failed to take basic steps to protect data from hackers and thieves, records show. In the latest example, the Office of Personnel Management is under fire for allowing its databases to be plundered by suspected Chinese cyberspies in what is being called one of the worst breaches in U.S. history. OPM repeatedly neglected to implement basic cybersecurity protections, its internal watchdog told Congress.

That story should worry every one of us, Democrats and Republicans alike. The AP referred to the massive cyber attack that recently struck the Obama administration as ''one of the worst breaches in U.S. history.'' But while this massive breach may have been ''one of the worst,'' it certainly—unless the administration can be rescued from the cyber security Dark Ages—will not be the last.

So the Senate will be considering bipartisan cyber security legislation this week that would help the public and private sectors defeat cyber attacks. The modern tools it contains, through the sharing of threat information, would provide for the construction of stronger defenses. The top Democrat on the Intelligence Committee says this bipartisan bill would also protect ''individual privacy and civil liberties.'' She is right. It contains strong measures to limit the use, retention, and diffusion of consumers' personal information. Information sharing with the government would also be voluntary under this bipartisan legislation.

No wonder my colleague from California joined virtually every other Democrat and every other Republican to endorse this bipartisan bill overwhelmingly in committee 14 to 1. No wonder this bipartisan bill is backed by a diverse coalition of supporters, too—everyone from the U.S. Chamber of Commerce to farm supply stores, to your local community bank.

This is a strong bipartisan, transparent bill that has been meticulously vetted by both parties in committee and that has been available online for literally months for anyone to read. My friend the Democratic leader has also publicly declared that the Senate could finish this bill in ''a couple of days.''

''In a couple of days,'' he said, ''at the most.''

So with cooperation, we can pass the bipartisan bill this week. There will also be an opportunity for Members of both parties to offer amendments. I urge colleagues who wish to do so to begin working with the bill managers right now.

This legislation is the work of many Members. I mentioned Ranking Member FEINSTEIN earlier, who has been a key player on this issue. I also wish to thank Chairman BURR for his strong leadership and his hard work across the aisle in developing this bipartisan bill. I urge the Senate to allow us to act and pass it this week.

The House of Representatives has already passed two similar White House-backed cyber security bills. The sooner we pass ours, the sooner we conference with the House to finally get a good cyber security law on the books, and the sooner our country can be better protected from more of these types of attacks.

NUCLEAR AGREEMENT WITH IRAN

Mr. MCCONNELL. Mr. President, this September, the Senate will formally weigh in on the nuclear deal struck between the White House and Iran. We will take a vote and answer a simple but powerful question: Will the agreement actually make America and its allies safer? When we do, the Senate, as an institution, will be put to the test.

● This ''bullet'' symbol identifies statements or insertions which are not spoken by a Member of the Senate on the floor.

Printed on recycled paper.

The first test will come in which answer we arrive at. Some might take the view that releasing billions of dollars to a state sponsor of terrorism while leaving the regime with thousands of nuclear centrifuges, an advanced research and development program, and the means to improve its full-spectrum warfighting capability would represent an acceptable outcome. Those Senators will vote one way.

Others will say that ending Iran's nuclear program is worth the necessary exertion of political leadership—leadership to keep the coalition unified, to reveal Iran's development of ballistic missiles and its support of terrorism, and to resolve the IAEA concerns over Tehran's refusal to allow access to nuclear scientists and facilities—because doing so would be in the best interests of our country and in the best interests of our allies. Those Senators will vote a different way.

In answering this fundamental question, every Senator will reveal his or her view of America's standing, its leadership, and its capabilities in the modern world. They will demonstrate whether they think these things can and should be brought to bear to defend our interests and to defend against Iran's aggressive expansion and its threatening nuclear program.

We know that the next Senate and the next President will continue to be faced with a threat posed by Iran. So we should conduct this debate with our eyes on the future. This is a critical test, but it is not the only one. The other test comes not in which answer we choose but in how we answer the question.

Can we join together to conduct a debate worthy of the importance of this agreement?

Can we call up the resolution and respectfully debate it without employing delay tactics designed specifically to impede the Senate's review of such a weighty matter?

Are Senators willing to focus on a matter of interest to the institution, defer committee activities, and sit in their chairs to truly listen and debate their colleagues on a matter of such significance?

Nearly every Member of both parties voted to have this debate when they passed the Iran Nuclear Agreement Review Act. Surely, Senators wouldn't then turn around and block a proper debate from even proceeding.

My hope is that the Senate could reach agreement to call up the appropriate resolution, reach agreement to allow ample time for Senators to express their views, and then proceed to a thorough, thoughtful, and respectful debate, because it is hard to overstate the importance of what we are about to consider: our role in the world, our commitment to our allies, the kind of future we will leave our children. It is all wrapped up in this issue.

The debate we will conduct deserves the appropriate and respectful deliberation that this body was designed to facilitate. Every Senator owes as much to this institution, and every Senator owes as much to this country and to the people we serve.

We may disagree on the first test, but we should all agree on the second one.

RECOGNITION OF THE MINORITY LEADER

The PRESIDING OFFICER. The Democratic leader is recognized.

NUCLEAR AGREEMENT WITH IRAN

Mr. REID. Mr. President, I agree with the Republican leader that we should work to come up with a way of proceeding in a dignified manner to this most important piece of legislation. Certainly, I would lend my efforts to try to get that done. It is easier said than done, with the feelings on both sides of the aisle on this issue and other issues.

CLEAN POWER PLAN

Mr. REID. Mr. President, yesterday President Obama took a very important step in addressing climate change and promoting clean energy. His Clean Power Plan is the strongest action ever taken by our government to fight climate change. The Clean Power Plan would reduce the dangerous amounts of carbon pollution being pumped into the atmosphere. By reducing pollution, the Clean Power Plan would yield significant public health benefits for our entire Nation.

Carbon pollution has many devastating effects on our environment, as well as the health and well-being of all of us. Sadly, pollution from burning fossil fuels disproportionately affects low-income people and families of color. Exposure to air pollution can aggravate preexisting health problems, especially respiratory maladies such as asthma.

For millions of Americans, carbon pollution affects their ability to breathe and exacerbates the problems they have with asthma. Consider these facts. Minority and lower income Americans are far more likely to live near coal-fired powerplants. Statistically, that is terribly accurate. African Americans are three times more likely to be hospitalized from asthma. African-American children have an 80-percent higher rate of asthma and are roughly three times more likely to die from asthma than their White peers. Roughly half of Latinos live in areas that frequently violate clean air rules, and Hispanic children are 40 percent more likely to die from asthma than non-Hispanic Whites.

In Nevada, just a short distance out of Las Vegas, about 35 miles, there is an Indian reservation. Approximately 30 years ago, NV Energy—Nevada Power—built this huge coal-fired generator there. Over the more than three decades it has been in existence, tens of millions of tons of coal have been burnt in that powerplant. It is a football field away from the reservation. Those Native Americans have been really sick as a result of that. Now there has been a court settlement that gives them a little bit of economic strength as a result of this, and, to its credit, NV Energy's new ownership has decided it is going to phase out that plant very quickly. That is good for the health of those Native Americans.

Today the plant is being decommissioned and solar is being built on the tribe's reservation. It is wonderful to see that. They have a lot of jobs, and it is giving some economic viability, in addition to the court settlement I just talked about.

President Obama put it best yesterday: ''If you care about low-income, minority communities, try protecting the air they breathe.'' That is exactly what the President's plan will do. It will clean the air we breathe, help curb health care costs, and improve the quality of life for all Americans. But that is not all.

As the plan is implemented, we will see even more investment in clean and renewable energy, which is not only good for the planet and our health, but it is good for the economy. The Clean Power Plan will boost renewable energy by 30 percent over the next 15 years, cutting pollution but, of course, creating tens of thousands of jobs for all Americans. President Obama's plan encourages programs and incentives to make American homes more efficient and lower consumers' utility bills.

Under the Clean Energy Incentive Program, a jump start in new jobs is expected from construction and installation of renewable energy and efficiency upgrades. This will incentivize new clean energy development and job creation before the new carbon standards even go into effect.

It has been disappointing, but not surprising, to see Republicans' knee-jerk opposition to addressing climate change. It is all the more frustrating because they have no plan of their own, except to let the smoke keep billowing. Instead, Republicans are clamoring to show special interests such as the oil baron Koch brothers how far they are willing to go to kill commonsense protections for our air and public health because it might hurt the bottom line of their coal and energy barons.

Last month, House Republicans passed legislation that would rescind President Obama's action addressing air pollution and climate change. Senate Republicans, for their part, are trying the same thing with policy riders in the Senate Interior and Environment appropriations bill.

Republicans would leave our children and grandchildren to pay the devastating costs of climate change. The Republicans have no solutions. They are afraid to acknowledge that climate change is a problem. It is.

President Obama's Clean Power Plan is good for this country. It is the

strongest action we can take today to ensure a cleaner, healthier tomorrow for our children and grandchildren, and it has to be done administratively. We can't get anything done legislatively. It is all opposed by the Republicans.

It would be good for my State of Nevada, where investment in clean energy is $6 billion. President Obama's plan gives States further flexibility to tailor programs for reducing carbon emissions while protecting public health and keeping electricity affordable and reliable.

Already the plan has wide support in Nevada. An article from the Associated Press yesterday reads:

> Several Nevada government business leaders plan to voice support for a federal campaign to limit carbon pollution from power plants around the nation in an effort to address global climate change. . . . Nevada Governor Brian Sandoval's energy chief, Paul Thomsen, says Nevada is well-positioned to comply with the first national limits on carbon dioxide from existing power plants.

Nevada understands the benefits clean energy brings to communities and the lives that will be improved by cleaning the air we breathe. Nevada is at the forefront of clean energy in the United States. Over the past decade, our clean energy infrastructure has expanded substantially, bringing good-paying jobs and new industries to Nevada. There can be no better place for President Obama to begin a dialogue with the Nation about the Clean Power Plan than Nevada.

I am looking forward to President Obama's visit to Nevada later this month to speak at the National Clean Energy Summit in Las Vegas on August 24. This is the 8th annual National Clean Energy Summit.

CYBER SECURITY

Mr. REID. Mr. President, we all want to address cyber security. Repeatedly, in the last two Congresses, I worked to convene the chairmen and ranking members of the relevant committees to move cyber security legislation, and we worked hard and came up with a number of bills, one of which we brought to the floor and was killed by the Republicans. What was good for our Nation's security was bad for the tea party and the Republicans. They blocked the cyber security legislation.

In this Congress, we have not been as uncooperative as the Republicans were when they were in the minority. Democrats are willing to proceed to the cyber security bill, if we can get assurance that Democrats can offer relevant amendments. It has to be done.

For the majority leader to say, as he did here today, that well, on this massive bill we had, I stuck the cyber security bill with a lot of other things—he knew it wouldn't work there. It was only to check it off his list that he tried to do it. Realistically, we have already been on this legislation. We should have been on this legislation. The Republican leader could have proceeded to cyber security instead of a politically motivated bill to defund access to health care for women. Unlike Republicans, we don't need all the poison pill amendments that deal with different subjects.

Democrats have amendments relevant to cyber security, and we must offer those. I have received a letter from Senators WYDEN, LEAHY, FRANKEN, WHITEHOUSE, and COONS yesterday that states:

> We understand that the Senate may soon consider the Cybersecurity Information Sharing Act. We share the view that increasing the security of U.S. networks while protecting Americans' privacy is an important goal, and while we have different views on this legislation, we are all interested in offering relevant amendments that we believe would improve this bill in various ways.
>
> We look forward to working with you to ensure that there is an adequate process for considering a reasonable number of amendments.

The way Republican Senators used to talk about an open amendment process, our request to have a few relevant amendments should be readily accepted by the Republicans. But then, looking at how the Republican leader has led the Senate this year, there is plenty of reason for Democrats to be concerned.

Just look at the bill the Senate just considered last week—a major highway bill with more than 1,000 pages. The Republican leader filled the amendment tree twice, not allowing any amendments to be offered. Accordingly, if you look at what the Congressional Research Service says, the Republican leader could potentially fill the amendment tree more times than any other majority leader has done in the first year of a Congress. So far he has done that more than I ever did.

Nevertheless, Democrats will work with Republicans to get on this bill and consider a reasonable number of important amendments. I hope the Republicans will cooperate with us.

Would the Chair announce the business of the day.

RESERVATION OF LEADER TIME

The PRESIDING OFFICER. Under the previous order, the leadership time is reserved.

MORNING BUSINESS

The PRESIDING OFFICER. Under the previous order, the Senate will be in a period of morning business for 1 hour, with Senators permitted to speak therein for up to 10 minutes each, with the majority controlling the first half and the Democrats controlling the final half.

The Senator from South Dakota.

REPUBLICAN-LED SENATE

Mr. THUNE. Mr. President, while Republicans were campaigning last fall, we promised the American people that if they put us in charge, we would get the Senate working again. That wasn't a campaign slogan. That was a commitment.

I am proud to report that we are delivering on that promise. The first 7 months of the 114th Congress have been some of the most productive the Senate has had in a long time. We have passed more than 70 bills to help strengthen our economy, reform our government, protect some of the most vulnerable, and strengthen our national security.

We passed bipartisan legislation to authorize the Keystone Pipeline, a valuable infrastructure project that would support more than 42,000 jobs during construction and invest $5.3 billion in the U.S. economy, all without spending a dime of taxpayer money.

We passed a bipartisan bill to strengthen our efforts to eradicate human trafficking in this country and to help its victims. This legislation, which passed the Senate with unanimous support from Democrats and Republicans and was signed into law in May, gives law enforcement new tools to target traffickers, including increased access to wiretaps, and it significantly expands the resources available to trafficking victims as they seek to rebuild their lives.

As negotiations with Iran over a nuclear agreement were repeatedly extended and as reports of significant compromises emerged, Democrats and Republicans alike grew concerned that the administration would fail to negotiate a deal that would be strong enough to prevent Iran from acquiring a nuclear weapon. To address these concerns, the Senate passed the Iran Nuclear Agreement Review Act. This legislation, which passed the Senate with overwhelming support from Democrats and Republicans and was signed into law by President Obama, was designed to ensure that the American people, through their elected representatives, would have a voice in any deal with Iran.

Without the Iran Nuclear Agreement Review Act there would be no opportunity for an up-or-down vote on this deal in Congress and no way to prevent the President from immediately waiving the sanctions that Congress put in place. Congress is currently reviewing the final agreement announced by the President, an agreement that has been greeted, I might add, with bipartisan skepticism. We will be holding a vote on this deal in September.

Increasing access to jobs and expanding opportunities for American workers is a priority of the Republican-led Congress. In May, with the support of 14 Democrats, the Republican-led Senate passed legislation to reauthorize trade promotion authority, which is key to securing trade deals that are favorable to American workers and businesses. Since 2009, increasing exports have accounted for more than 1.6 million new jobs in the United States.

Manufacturing jobs that depend on exports pay an average of 13 to 18 percent more than other jobs in the economy. Thanks to the bipartisan trade promotion authority legislation, the administration now has a key tool to negotiate trade agreements that will create more good-paying jobs for American workers and open new markets for products labeled ''Made in the U.S.A.''

After taking up bipartisan legislation to protect our economy, the Senate turned to another key Republican priority; that is, supporting our military men and women. The National Defense Authorization Act, which we considered in June, passed the Senate with strong bipartisan support. In addition to authorizing the funding our military needs to defend our Nation, this bill contains a number of reforms that will expand the resources available to our military men and women and strengthen our national security.

Among other things, this legislation targets $10 billion in unnecessary spending and redirects those funds to military priorities such as funding for aircraft and weapons systems and modernization of Navy vessels. It implements sweeping reforms to the military's outdated acquisitions process by removing bureaucracy and expediting decisionmaking. That will significantly improve the military's ability to access the technology and equipment it needs. It replaces the outdated military retirement system with a modern system that will extend retirement benefits to 75 percent of our servicemembers.

During the month of July, the Senate built on its bipartisan achievements with two important pieces of legislation: the Every Child Achieves Act and the DRIVE Act. The Every Child Achieves Act, which passed the Senate by an overwhelming margin, reauthorizes Federal K–12 education programs and revokes problematic Federal mandates such as those that resulted in the phenomenon of overtesting. This legislation restores control of education to those who know students the best, such as parents, teachers, and local school boards.

The DRIVE Act, which passed the Senate by a strong bipartisan margin, is notable because it is the first Transportation bill in almost a decade to provide more than 2 years of funding for our Nation's infrastructure needs. Around the country, hundreds of thousands of people and hundreds of thousands of jobs depend on the funding contained in Transportation bills. When Congress fails to provide the necessary certainty about the way transportation funding will be allocated, States and local governments are left without the certainty that they need to authorize projects or make long-term plans for transportation infrastructure. That means that essential construction projects get deferred, necessary repairs may not get made, and jobs that depend on transportation are put in jeopardy. The DRIVE Act will give States and local governments the certainty they need to plan for and commit to key infrastructure projects.

Every bill I have discussed today passed the Senate with strong bipartisan support. One major reason for that is Senate Republicans' commitment to opening up the legislative process here in the Senate. Under Democratic control, the legislative process of the Senate had almost ground to a halt. Instead of being developed in committee, bills were frequently drafted behind closed doors, and not only the minority party but many rank-and-file Democrats were shut out of the process.

When Republicans took control of the Senate in January, we changed all that. We opened up the committee process and debate on the floor. We made it a priority to ensure that every Senator—every Senator—both Democratic and Republican, has an opportunity to make his or her voice heard. During 2014, the Democratic leadership allowed just 15 amendment rollcall votes in the entire year—2014. Republicans allowed more than 15 amendment rollcall votes in our first month. So far this year, we have allowed more than 165 amendment rollcall votes, and we still have 5 months to go in the year. The Republican-led Senate has accomplished a lot over the past 7 months. But we know that we have a lot more to do.

As the 114th Congress continues, we will continue to fight for the American people's priorities. We hope the Democrats here in the Senate will continue to join us.

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

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

CYBER SECURITY

Mr. DAINES. Mr. President, as I like to say, there are only two types of companies: those that have been hacked and those that know they have been hacked. This was recently seen at JPMorgan Chase. Last summer the company suffered a cyber attack that involved the theft of contact information for about 76 million households. In the aftermath, JPMorgan Chase is expected to double its budget for cyber security efforts this year. But the case of JPMorgan is not unique nor a simply cautionary tale for other major companies.

In the last few months, we have seen one of the largest cyber attacks on our Nation's technology infrastructure and other major cyber breaches affecting our financial and transportation sector. I share these comments in the context of having worked as an executive for a cloud computing company for 12 years prior to serving in the Senate. In the midst of these attacks, we see radical Islamic terrorists infiltrating American social media networks to recruit Americans to join them as jihadists overseas.

We must work to address these challenges, and our response must be measured as well as thoughtful, not only about the immediate threats to our cyber infrastructure but also to the long-term effects on our national security and our constitutional freedoms. As we are seeing with the European Union, after years of debate, the EU is currently working on a policy to ensure their citizens are notified of cyber breaches within 72 hours and that victims of these attacks are notified without undue delay.

This is the type of response we need in the United States, much like the notification reforms that I have worked for in Congress. On a near daily basis, we see headlines in our major newspapers that underscore the absolute importance of creating a concrete timeline for implementing timely notification standards.

Having spent more than 12 years working on technology, I know firsthand the power that Big Data holds. I also understand the importance of setting standards and clear guidelines. As we always said in 28 years of business, if you aim at nothing, you will hit it. It is important that we not only expect more but that we also inspect. We want to be assured that guidelines are being followed.

It is unacceptable that any American is left in the dark when their personally identifiable information or PII may have been breached. That is why I have been fighting to strengthen notification requirements and ensure that the American people know when their personal information is compromised. When I was running customer service operations at RightNow Technologies and looking out for our customers, when we had a problem, our policy was that we notified our customers as soon as we were aware of the problem. Maybe we did not always understand the magnitude at the time of the problem, but we believed we owed it to our customers to get back to them as soon as possible.

The customers, the consumers of this country, should be served in a similar way. But as the Senate prepares to consider cyber security reforms, we also need to strike the right balance between protecting our cyber security infrastructure and the personal information of Americans, while also protecting the constitutional rights and the liberty of the American people. We must protect our Nation's security while also preserving our civil liberties.

We must remain vigilant. We must ensure that we have robust and transparent debate about cyber protection and what reforms must be implemented to protect American civil liberties. We

see some of these protections in the legislation I cosponsored, spearheaded by Senators MIKE LEE and PAT LEAHY. The Electronic Communications Privacy Act Amendments Act of 2015 modernizes our Nation's electronic privacy laws and brings protections against warrantless searches into harmony with the technological realities of the 21st century.

The protections currently on the books may have been robust in 1986 when the ECPA was written, but they do not adequately defend our citizens against the mass data storage that currently exists. Nobody in 1986 would have ever envisioned where we are today as to the massive amount of data that is collected and stored today on the American people. This bill ensures that the Federal Government gives our law enforcement officials the tools they need, while ensuring that Montanans and the American people are not subjected to invasive and unwarranted searches.

Privacy and security both matter. I believe we can find a balance that protects both. I urge my colleagues to join me in finding reforms that stop cyber criminals from infiltrating our security networks and also preserve the privacy and the civil liberties that Montanans and Americans hold dear.

THE ADMINISTRATION'S CLEAN POWER PLAN AND COAL

Mr. DAINES. Mr. President, I would like to shift gears for a moment and share some comments about President Obama's news that he made yesterday with the EPA. Yesterday, President Obama and the ''Employment Prevention'' Agency, the EPA, continued to wage their war on American energy, American families, and American jobs. As President Obama was announcing his plan to devastate Montana's coal industry and the good-paying jobs it provides, yet another coal company filed for bankruptcy.

At the same time, the J.E. Corette powerplant, in my home State of Montana in Billings, is being dismantled as we speak in the aftermath of President Obama's previous anti-coal regulation. In addition to supporting 30 jobs, the Corette powerplant has powered tens of thousands of Montana homes and contributed several million dollars in tax revenue to Montana and Yellowstone County every year.

Over the past year, Montanans have braced themselves for the release of the Obama administration's final regulations, which were already set to wreak havoc on our coal industry and make construction of any new coal-fired plant virtually impossible. The proposed rule was bad. The final rule is even more devastating to Montana jobs and to Montana families.

The final rule announced by the Obama administration makes the retirement of existing coal-fired powerplants inevitable within the next few decades.

The rules moved the goalposts and, I might add, to the wrong end of the field. These rules will most likely lead to the shuttering of Montana's Colstrip Power Plant and countless others across the Nation. It would be devastating for our economy and hard-working families across the State.

Energy rates will increase. Thousands of Montana family-wage jobs would be lost. Critical tax revenue for schools, for our teachers, roads, and our infrastructure would evaporate. In the Obama administration's final rule, they took an already bad rule and they made it worse.

The so-called Clean Power Plan forces Montana to achieve even more aggressive standards than originally proposed. According to POLITICO, in 2012 Montana produced 2,481 carbon pounds per megawatt hour.

Under the President's plan, by 2030, he wants Montana to produce only 1,305 carbon pounds per megawatt hour. That is a 47.4-percent reduction in Montana's carbon emissions because in Montana more than half of our electricity comes from coal. In fact, my mobile device is powered by coal. Coal also powers good-paying jobs for thousands of Montanans, including Montana tribal members and union workers, and generates nearly $120 million in tax revenue every year.

America is poised to lead the world's energy needs, but this will be done through American innovation, through American ingenuity, not more regulations. The Obama administration's regulations are completely out of touch with global realities, and this is why: Global demand for coal-fired energy will not disappear, even if the United States shuts down every last coal mine and coal-fired powerplant.

Nations such as China, Korea, and Japan will continue using coal as it is reliable and it is affordable. These nations should be powered by cleaner Montana coal because the coal we produce in Montana is cleaner than Asian coal.

In terms of the environmental picture for the world, we are better off using American coal, Montana coal—not coal from Asia. Rather than dismissing this reality, the United States should be on the cutting edge of technological advances in energy development and leading the way in promoting the use of clean, affordable American energy.

In fact, according to the International Energy Agency's 2013 data, the world consumes about 6 billion metric tons of steam coal for power generation. Of that, the United States consumes 750 million metric tons.

Let's put that into apples-to-apples comparison. That means the United States consumes about 12 percent of the coal. The rest of the world consumes 88 percent. As the world sees an increased demand for power, it is clear we need to be leading the way in clean coal and energy innovation.

The United States should be leading. Let's be working toward clean coal, clean energy, and leading the world as our 12 percent could have an influence on the other 88 percent.

America, we can and we should power the world, but we could only do it if the Obama administration steps back from its out-of-touch regulations and allows American innovation to thrive once again to not only lead America but to lead the world.

I yield back the remainder of my time.

The PRESIDING OFFICER. The Senator from Indiana.

WASTEFUL SPENDING

Mr. COATS. Mr. President, last week I delivered my 19th ''Waste of the Week'' and we actually reached our goal of $100 billion in savings for the taxpayer by identifying waste, fraud, and abuse. This was money spent by the Federal Government, money collected from hard-working earners who paid their taxes, sent them to Washington, and expected they would be used for essential purposes, such as providing for our national security, supporting research at NIH for medical advances that would provide lifesaving techniques and medicines to Americans, funding the rebuilding of crumbling bridges and highways, and any number of things the Federal Government is involved in that the American public agrees are essential functions that could be performed only by the Federal Government.

What we want you to do though, they are saying, is be as efficient as you can. If there is excess money wasted on programs that have no place in the Federal budget, let's identify those, let's eliminate those, and either return our tax money and lower our tax rates or use it for something more essential.

We have reached our goal of $100 billion of waste, fraud, and abuse identified by nonpartisan agencies—not Republican agencies, not Democratic agencies or firms but nonpartisan agencies—that simply look at numbers, identify the projects, identify the spending, and ask the question: Do we truly need to do that?

Particularly at a time when the deficit clock keeps ticking, when we continue year after year after year to spend more than we take in, despite raising taxes, despite looking for ever more sources of income, it is clear we need to take the necessary steps not to spend more than is absolutely necessary to function on behalf of the American people.

So today I am on the floor for speech No. 20. We reached the goal. It is just the beginning of August. The Senate has many more weeks in front of it, but we are going to keep going because it is amazing the amount of waste, fraud, and abuse that has been identified by some of these nonpartisan groups looking at Federal expenditures. If we can add to our chart, I think we will have to add an extension to that chart or devise another one—

perhaps put another gauge over here—because we are going to keep doing this every week the Senate is in session.

Today, as I said, we are looking at No. 20. I looked at two agencies that exist in the Federal Government: the National Endowment for the Humanities, NEH, and the National Endowment for the Arts, NEA. These two agencies are engaged in cultural projects. Some of these are—people would deem—somewhat essential, but we have looked at two agencies that we think ought to be identified today.

The public probably will remember the 87th Academy Awards—better known as the Oscars—that took place in Hollywood a few months ago. Many Americans tune in and watch this high-profile event featuring America's rich and famous. As always, a parade of actors pull up in their stretch limousines and step into the bright lights of the entertainment industry's media—the flashing lights, the march down the red carpet, and stop to have their pictures taken. There, in tailored tuxes and designer gowns—some of which cost, amazingly, over $100,000—everybody is trying to outdo everybody else.

The bottom line is Hollywood is not short of money. As Americans watch this, they see the Oscars that are being offered. Then we look at that and say: What in the world is a $25,000 check from the Federal Government to Hollywood doing in this process?

It is hard to understand the concept that Hollywood needs support, needs a handout from the Federal Government, but they are developing an Academy Museum of Motion Pictures in Hollywood. Somehow they have applied for a $25,000 grant from the National Endowment for the Arts. Now, that is not a major amount compared to our budget problems here and the money we deal with, but the American public ought to be saying: Why in the world are we giving a penny to Hollywood to support the building of a museum?

It is simply because the process is open for anybody to submit for a grant. But who is reviewing these things? Who is looking at this? Does Hollywood truly need taxpayer money to construct a museum of motion pictures through the National Endowment for the Arts?

We also discovered that the National Endowment for the Humanities got engaged in one of these efforts, spending considerably more—$914,000—to support a conference entitled ''What is Love? Romance Fiction in the Digital Age.'' The conference was full of speakers networking with each other and even giving the opportunity for adults to design and color their own title page.

Again, I am asking why. Why, given our $18.5 trillion debt growing every day, do we have to give away a nearly $1 million grant to support a conference on how in the digital age to develop romantic books?

While it might be fun to go deeper into this and examine just exactly what goes on at this conference, that is not really why I am speaking on the floor today. I am simply here to ask why. Is this necessary? Is this the kind of thing we need to be supporting and doing with hard-earned taxpayer dollars that are sent to Washington, not for these purposes?

So today, the cumulative runs close to $1 million—$939,000—of taxpayer savings that would go onto our gauge, and we add yet another increment to the gauge in determining how tax dollars are spent.

We are going to continue doing this. This is a small one today. You can see we had some major chunks and major dysfunctions in the Federal Government, but I think it is important for every Senator to be able to go home, talk to their people, and say: We are making every possible effort we can to be efficient and effective with the money you sent to Washington, and we are looking into every dollar to make sure it is spent on essential functions of the Federal Government.

It is astounding how much is being sent, used, and wasted, how much fraud and waste takes place. We will continue to identify that each week.

That is our waste of the week. We will be back each week after our August recess when the Senate is in session to continue to identify ways in which we can save the taxpayers' money.

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

The PRESIDING OFFICER (Mr. FLAKE). Without objection, it is so ordered.

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

The PRESIDING OFFICER. The Senate is in morning business.

FOR-PROFIT SCHOOLS

Mr. DURBIN. Mr. President, I have come to the floor many times to talk about for-profit colleges and universities. This is a problem and a challenge we face. What you need to know are three numbers to understand the for-profit college and university industry in America.

By way of preface, this is the most heavily subsidized private business in the United States of America. What are we talking about? The largest, the University of Phoenix; Kaplan University; DeVry University; Rasmussen; Corinthian—you have heard all the names because they advertise constantly, and the money they use to advertise comes from Federal taxpayers.

There are three numbers—and if I were a college professor or law school professor, I would say this is going to be on the final—on for-profit colleges and universities. Ten percent of high school graduates attend for-profit colleges and universities—10 percent. Twenty percent of all the Federal aid to education goes to for-profit colleges and universities. Why so much? They charge so much. Their tuition is so high. Ten percent of the students; 20 percent of the Federal aid to education; 44 percent of all the student loan defaults in America are at for-profit colleges and universities. Ten percent of the students, 44 percent of the defaults. Why? They charge so much that the students can't finish their education or they end up with a worthless diploma. That is the reality.

There is a second reality. This industry is in serious economic trouble. Last week we had news of another Federal investigation of a for-profit college. In a filing with the Securities and Exchange Commission, the University of Phoenix—the largest for-profit college and university—revealed it is under investigation by the Federal Trade Commission for unfair and deceptive practices.

This news comes just weeks after the Center for Investigative Reporting published a story about the University of Phoenix's thinly veiled, dubious marketing and recruiting efforts on military bases—exploitation of our men and women in uniform. Over the past several years, the University of Phoenix has spent millions of dollars to sponsor events, including dances, parties, and concerts, on military bases. Is it because they love our men and women in uniform? No. It is because they want to sign them up. To the University of Phoenix, these sponsorships were simply advertising and marketing events to enroll more men and women in uniform.

When you serve our country, we show our appreciation by saying there is a GI bill waiting for you at the end of your service—in fact, in some cases, while you are still serving—and for your family, too, so that you will be prepared after you have served our country to have a good life with good education and training and job opportunities.

These for-profit colleges and universities can smell an opportunity to make even more money. The University of Phoenix is after these men and women in uniform. They are after tuition assistance dollars. TA is a program that provides up to $4,500 a year, so servicemembers can use it toward a postsecondary education. And guess what. The money isn't counted in the Federal 90/10 calculation that caps the amount of money these for-profit schools can receive from the Federal Government. Did you hear that? Ninety percent of their revenue comes from the Federal Government. That is why for-profit colleges and universities are the most heavily subsidized private for-profit businesses in America. To for-profit colleges, the money from servicemembers and veterans is unlimited

money. All they have to do is sign them up. And that is what they are doing with these sponsorships.

After the article was published, I wrote to Secretary Ash Carter—Department of Defense—to ask him to take action. The University of Phoenix reportedly is in clear violation of Executive orders limiting the access of these schools to our men and women in uniform. The Department of Defense has confirmed to me they have opened an inquiry into the matter.

During the Senate's reconsideration of the National Defense Authorization Act, I filed an amendment to require the Department to post information on Federal and State investigations and lawsuits against schools on its online education resources for servicemembers.

As part of the Tuition Assistance Program, the Department of Defense has created what it calls TA DECIDE. This allows servicemembers to find information about specific schools when deciding where to use their tuition assistance benefits. It includes information such as the graduation and default rates. Do you know why? Because once that servicemember has used up that GI bill, it is gone. If they waste it on one of these for-profit colleges and universities that give them little or nothing for their GI bill, they do not get a second chance.

Of course, servicemembers need accesses to this information. Publicly traded companies such as the University of Phoenix have to disclose the information to the SEC when they are under investigation. Members of the military should know that, as well as the general public. It only makes sense.

My amendment wasn't taken up during the Senate's debate, but last week 12 Senators joined me in writing Secretary Carter. This commonsense step to ensure better information for servicemembers about their education options is one the Department of Defense needs to make.

I also want to say a word about another for-profit college that is notorious for its exploitation of students—Ashford University. Ashford University first came to my attention when former Senator Tom Harkin of Iowa had an investigation. He took a look at this so-called university in his home State of Iowa. Do you know what he found? He found they had purchased a small Catholic girls college, purchased their accreditation, and then reopened it under the name ''Ashford University.'' Do you know how many faculty members there were at Ashford? One faculty member for every 500 students. It wasn't a real university; it was an online scam. They announced last week they are closing down their campus in Iowa. What a heartbreak that must be for the people of Iowa—to lose such a stalwart higher education citizen. That is the reality.

I have run into students in Illinois who said they had just graduated from college.

I said: Where did you go?

They said: Ashford.

And I thought, oh my goodness. What a disappointment. You have wasted your time and your money, you are deep in debt, and that diploma, sadly, is worth very little.

The tide is turning against the for-profit colleges and universities. The question is whether this Senate, this Congress, this government will step up once and for all and defend those young men and women who are wasting their time and money and taxpayer dollars—and in many cases GI bill benefits—on these worthless for-profit schools.

It is time for us to wake up to this reality. I am glad to see this industry is finally facing its day of reckoning.

Mr. President, I yield the floor.

The PRESIDING OFFICER. The Senator from Massachusetts.

SCHEDULES THAT WORK ACT

Ms. WARREN. Mr. President, I come to the Senate floor today to talk about something that has been bothering me. Who is this Senate supposed to be working for? For years now, this economy has been great for those at the top, but for everyone else, it is getting harder and harder to make it from paycheck to paycheck, harder and harder to build any real security. The world is changing, and Congress can make decisions that help working people stay in the game and help level the playing field or we can just turn our backs.

What have the Republicans done over the past 6 months to try to make families a little more secure, to give people a fighting chance? What have they done? They have turned their backs. In the past 6 months, they have burned huge amounts of time as they tried to shut down Homeland Security, tried to build a pipeline to help a Canadian oil company, tried to turn a human trafficking bill into a referendum on abortion, and now tried to defund Planned Parenthood—all this instead of working on the kinds of issues that would help level the playing field for hard-working people.

You know, there is a lot we could do. For example, Democrats have been fighting to raise the minimum wage. And I strongly agree that no one—no one—should work full time and still live in poverty. I think a $7.25-an-hour minimum wage is disgraceful. I support the Federal bill to raise the minimum wage to $12 by 2020, and I applaud the fight for $15 that is springing up across this country.

When I am asked about whether we should raise the minimum wage, I have three answers: Yes. Yes. Yes. But raising the minimum wage is only the beginning. Half of low-wage workers have little or no say over when they work, and an estimated 20 to 30 percent are in jobs where they can be called in to work at the last minute.

I want us to think about what this means for someone who is busting her fanny trying to build some economic security. Imagine trying to plan for anything—for childcare, for going back to school, for getting a second job—without knowing when you will be working next week. Imagine trying to plan a monthly budget when your work hours and paycheck can fluctuate 70 percent in a single month. Imagine trying to schedule a doctor's visit or parent-teacher conference if you could get fired just for asking for a few hours off. This is the real world of millions of workers who struggle to make ends meet.

This is something we can fix. A few weeks ago, I introduced the Schedules That Work Act, with 17 Democrats in the Senate and more than 60 Democrats in the House of Representatives. The bill is just common sense and basic fairness: A single mom should know if her hours are being canceled before she arranges for daycare and drives halfway across town to show up at work, a young man trying to put himself through school should be able to request a more predictable schedule without getting fired just for asking, and a worker who is told to wait around on call for hours with no guarantee of work should get something for her time.

The Schedules That Work Act does two simple things: First, it gives all workers the right to request a change in their schedule without getting fired just for asking, and, second, it gives workers who face the worst scheduling practices—workers in retail, food service, and cleaning workers—2 weeks' notice of their work schedules and some additional pay if they are required to wait on call but don't get any work.

Now, look, this bill recognizes that there are emergencies, and when employers have unexpected needs they can reschedule their workers, but we are asking for a little basic fairness so that in ordinary times—day-by-day, week-by-week—workers will have a stable schedule and a chance to build some real economic security.

Democrats want to get to work on changes in the law that would give working people a fighting chance. We want Republicans to let us take up these proposals and let us vote on them. Instead, Republicans are pushing a different agenda, focusing on defunding women's health care and protecting those at the top.

People say Washington doesn't work, but that is wrong. Washington works great—for the right people. When the corporate lobbyists want a carve-out or giveaway, when a giant oil company wants the Keystone Pipeline or when Citibank wants to blast a hole in Dodd-Frank, Republicans fall all over themselves to make it happen. When the rightwing wants to cut off access to health care, Republicans are ready to go, but when it comes to the things that will help families, they turn their backs. This has to stop. We are not here to work for the lobbyists. We are not here to make life easier for big oil companies or for big banks. We are

here to make this country work for hard-working Americans. That is our job, and it is time for this Republican Senate to start doing that job.

Let's take up and pass the Schedules That Work Act. Let's give working families a fighting chance to build a future.

I yield the floor.

The PRESIDING OFFICER. The Senator from Iowa.

MARINE CORPS AUDIT

Mr. GRASSLEY. Mr. President, yesterday a very important Government Accountability Office report came out. I am going to present my view of that report in a little bit backward way by giving a summary before I speak about the fine points of this report.

Broken bookkeeping has plagued the Pentagon for years. Under deadline pressure, the Marine Corps claimed to be ready for a clean audit. An outside auditing firm produced work papers in support of an opinion on a clean audit that employees in the Defense Department inspector general's office found lacking. However, a manager in the inspector general's office overruled his lower level colleagues. That resulted in the inspector general's release of a clean opinion on the audit of the Marine Corps.

Meanwhile, work papers began to creep out of the bureaucracy showing the unsupported basis for such a clean opinion. The inspector general was then forced to withdraw that opinion.

Now the Government Accountability Office is releasing a report that exposes the whole house of cards. One senior employee with an apparent bias toward the outside auditing firm led his agency down the wrong path. We need to get things back on track and prevent an embarrassing setback like this from ever happening again.

I will go into those details. As I often do, I come to the floor to speak about the latest twist in the 25-year struggle to fix the Defense Department's broken accounting system. Billions have been spent to fix it and achieve audit readiness, but those goals remain elusive. Defense dishes out over $500 billion a year. Yet the Department still can't tell the people where all the money is going, and now the drive to be audit-ready by 2017—that is what the law requires—has taken a bad turn and become a fight over the truth.

As overseers of the taxpayers' money, we in Congress need to get the Audit Readiness Initiative back on track, moving forward in the right direction.

I last spoke on this subject a long time ago—December 8, 2011. On that occasion, I commended the Secretary of Defense, Leon Panetta, for trying to get the ball rolling. He wanted to halt endless slippage in audit deadlines. He wanted to provide an accurate and regular accounting of money spent to comply with the constitutional requirements. He turned up the pressure and in effect drew a line in the sand.

He directed the Department to, in his words, ''achieve partial audit readiness,'' with limited statements by 2014, and, in his words, ''full audit readiness'' with all-up statements by the statutory deadline of 2017.

Not one of the major DOD components—including the Army, Navy, Marine Corps, and Air Force—reached Leon Panetta's 2014 milestone. None was or is audit ready today.

That said, one component—the Marine Corps—stepped up to the plate and claimed to be ready for what Leon Panetta's goal was. To test that claim, the accounting firm Grant Thornton was awarded a contract to audit five Marine Corps financial statements, 2010 to 2014.

The first two, 2010 and 2011, were unsuccessful. The Marine Corps was not ready. The third one was the 2012 audit, which is finally finished.

The 2012 audit was put under a microscope and subjected to intense review by the Office of Inspector General along with two other independent watchdogs.

The Marine Corps audit was a disaster. First, it took an ugly turn. It got twisted out of shape and turned upside down. Now it is getting turned right side up, thanks to the Government Accountability Office.

Grant Thornton was required to produce a conclusion memorandum. This happens to be what we might call a quasi-opinion. Work was to be finished by December 2012, but it took an extra year. So right off the bat it was running into trouble. The scaled-down financial statement did not meet contract specifications. So this was a showstopper that got glossed over. The contract was modified to accept a makeshift compilation that was cobbled together. It is called a Schedule of Budgetary Activity. It covers only current year appropriations and not vast sums of prior year appropriations that are still lost in the statutory and money pipeline. Of course, that is a far cry from a standard financial statement.

Even reducing the scope of the audit wasn't enough to overcome all of the other problems. The Office of Inspector General audit team was responsible for issuing the final opinion. After completing a review of Grant Thornton's workpapers in early 2013, the team determined that the evidence presented did not meet audit standards. It concluded that an adverse opinion—or what they call a disclaimer—was warranted. The team's rejection of Grant Thornton's conclusions embroiled the opinion in controversy and foul play. The trouble began when the Deputy IG for Auditing, Mr. Dan Blair, intervened and reportedly overruled his team's conclusions. He issued an unqualified or clean opinion that was not supported by the evidence in the workpapers—quite a showboat approach.

Despite mounting controversy about the validity of the opinion, Secretary of Defense Hagel rolled out that opinion December 20, 2013—with trumpets ''ablast.'' At a ceremony in the Pentagon's Hall of Heroes, he gave the Marine Corps an award for being the first military service to earn a clean opinion. The Assistant Commandant of the Marine Corps, Gen. John Paxton, accepted the award. According to press reports, he did so with ''reluctance. . . . He mumbled something, then bolted from the stage at flank speed.'' Why would General Paxton take off like a scalded dog? Was it because he sniffed a bad odor with this so-called clean report and all the colorful presentations that were made by Secretary Hagel?

At that point, the word was already seeping out: The opinion was allegedly rigged. I heard rumblings about it and began asking Inspector General Rymer questions. Because of all the controversy, we asked his independent audit quality watchdog, Deputy Assistant IG Ashton Coleman, to review the audit. Mr. Coleman sent Inspector General Rymer reports in October 2014 and May of this year. These reports ripped the figleaf clean off of Mr. Blair's charade. They reinforced the audit team's disclaimer. After recommending ''the OIG rescind and reissue the audit report with a disclaimer of opinion,'' Mr. Coleman zeroed right in on the root cause of the problem. That root cause was impaired independence. In other words, the people involved in this charade had an agenda that wasn't about good handling of the taxpayers' money, it was protecting somebody.

Mr. Coleman concluded that Mr. Blair ''had a potential impairment to independence.'' He and a Grant Thornton partner, Ms. Tracy Porter Greene, had a longstanding but undisclosed professional relationship going back to their service together at the Government Accountability Office in the early 1990s. According to Coleman, that relationship by itself did not pose a problem. However, once it began to interfere with the team's ability to make critical decisions, he said it created an appearance of undue influence. Coleman identified several actions that led him in this direction.

The appearance problem was framed by a four-page email on August 2, 2013, from Ms. Greene to Mr. Blair but seen by the team and others, including me. It was a stern warning. If a disclaimer was coming—and Ms. Greene knew it was—she wanted, in her words, ''some advanced notice.''

She needed time then, as she thought, to prepare the firm's leadership for the bad news. A disclaimer, she said, would pose ''a risk to our reputation.'' At the email's end, she opened the door to private discussions to resolve the matter.

The record clearly indicates that both Blair and Greene began holding private meetings—without inviting Contracting Officer's Representative Ball and the Office of Inspector General team to participate in those discussions. Both believed the contracting

officer's representative and the team were—in the words of Greene and Blair—''biased toward a disclaimer rather than considering all the facts.'' I attributed those words to Greene and Blair, but those were Mr. Blair's words.

This shows how the independence of the audit and the review of the audit were questionable. To put these actions in perspective, I remind my colleagues that the inspector general was exercising oversight of the company's work. The inspector general needed to keep top company officials like Ms. Greene at arm's length, and holding private meetings with Greene wasn't the way to do it. These meetings may have violated the contract.

Why would the top IG audit official prefer to hold private meetings with Ms. Greene? Why would he seem so willing and eager to favor the firm over his team—even when the evidence appeared to support the team's position? Why would he favor the firm over the evidence and over the truth? Why would he admit on the record that ''OIG auditors were not independent of Grant Thornton''? Why would he order the team to give the work papers to the firm so they could be ''updated to reflect the truth''? The firm was not even supposed to have those documents, so we get back to impaired independence again.

Coleman cited other indications of this impaired independence. Contracting Officer's Representative Ball had rejected the firm's 2012 deliverables because they were ''deficient.'' They did not meet quality and timeliness standards. The deliverables in question were the company's final work product, including the all-important quasi-opinion called a conclusion memorandum.

This posed a real dilemma. Until she accepted the 2012 deliverables, the follow-on 2013 contract with Grant Thornton could not be awarded, and Blair wanted it done yesterday.

The impasse was broken with a crooked bureaucratic maneuver. A senior official, Assistant Inspector General Loren Venable, provided a certification that there were no major performance problems and Grant Thornton had met all contract requirements. Just then, with the stroke of a pen, that deceptive document cleared the way for accepting the disputed materials, paying the firm all their money, and awarding them at the same time a follow-on contract. Yet the record shows that even Mr. Blair admitted that ''we accepted deficient deliverables.''

Why would a senior Office of Inspector General official attempt to cover up a major audit failure by Grant Thornton in order to reward the poorly performing company with more money and a new contract? For a series of audit failures, the firm got paid $32 million.

These actions appear to show how undue influence and bias trumped objectivity and independence. Alleged tampering with the opinion may be the most flagrant example of impaired independence.

While the team identified major shortcomings with Grant Thornton's work and disagreed with its conclusions, the team was blocked from exercising its authority to issue a disclaimer. So where is the independence? Instead, that team was forced to do additional work in a futile attempt to find evidence to match the firm's conclusion, but there was no such evidence.

Two weeks after Ms. Greene's email warning that a disclaimer could destroy the company's reputation, the front office resorted to direct action. With the team's disclaimer staring him in the face and with complete disregard for evidence and standards, Mr. Blair gave the Office of Inspector General team a truly stunning set of instructions. These were as follows: No. 1, the Marine Corps earned a clean opinion; No. 2, Grant Thornton has supported a clean opinion; and No. 3, do what it takes to reach the same conclusion as Grant Thornton.

In the simplest of terms, this August 14 edict says: There will be a clean opinion. Disregard the evidence. Figure out how to do it and make it happen.

These instructions provoked an internal brawl. The team manager, Ms. Cecilia Ball, balked. She stated flatout:

> I cannot do that. Our audit evidence does not support an unqualified [clean] opinion. We are at a disclaimer.

She wanted justification for Mr. Blair's decision to overturn the team's opinion. She asked:

> Show me where my work is substandard and where my conclusions are incorrect. And I want to know what standards Mr. Blair used to reach his conclusions.

She never got a straight answer. From that point on, it was all downhill. When the team ignored coaxing, they got steamrolled.

Mr. Blair attacked their competence, professionalism, and independence. He repeatedly accused them of being ''biased.'' The team's top manager, Ms. Cecilia Ball, reacted to the abusive treatment. She said:

> I don't appreciate the accusations to my professionalism and my team's. I don't think we are the right fit as our integrity is being questioned.

She later quit the team in disgust.

In early December, just as the clean opinion was about to be wheeled out, Ms. Ball made one final request for explanation: Why was ''the team's disclaimer of opinion not the correct opinion''? We repeatedly documented and explained why Grant Thornton's conclusion was unsupportable. ''The vast knowledge of the Front Office could have provided us insight as to where the team's logic was flawed.''

In this case, the front office was unwilling to consider anything other than a clean opinion. These words are from the horse's mouth. The clean opinion was handed down from on high. The front office was Mr. Blair's domain.

All of these actions, when taken together, appear to show a lack of independence and a flagrant disregard for audit ethics, audit standards, audit evidence, and accepted practices.

In his oversight role, Blair had a responsibility to be independent, objective, and professionally skeptical. If the firm's work failed to meet standards, as it did, then he had a responsibility to face the truth and tell it like it is. He needed to be a junkyard dog and issue the disclaimer. Maybe he lost sight of his core mission and turned into a Grant Thornton lapdog. It sure looks that way.

Mr. Blair's words, deeds, and prior association with the Grant Thornton partner, Ms. Greene—when coupled with their many emails that were widely distributed—gave the appearance of undue influence by the Grant Thornton partner. The tone and the substance of the Blair-Greene emails suggest a professional relationship that was just too cozy—a relationship that might have been wise to disclose according to audit standards and professional ethics.

Inspector General Rymer disagrees with Mr. Coleman's findings of impaired independence. However, Mr. Rymer's evidence does not square with evidence presented by Coleman. For these reasons, Senator JOHNSON of Wisconsin and I will be asking the Comptroller General—the guardian of government auditing standards—to review all relevant evidence. Since independence is a cornerstone of audit integrity, we must be certain it has not been compromised.

Now, just yesterday another blockbuster report has been rolled out. The Government Accountability Office has issued a highly critical report. It was prepared at the request of Senator JOHNSON, Senator MCCASKILL, and Senator CARPER. The Government Accountability Office report is thorough and competent and tells the story as it happened.

Over the last 2 years, the GAO team held endless meetings with the Office of Inspector General, including Jon Rymer and Dan Blair. So the IG has known for some time what was coming down the pike. They knew early on the GAO report concluded that the evidence in the workpapers did not support the clean opinion of the Marine Corps audit.

Echoing Ms. Ball's unanswered pleas, the Government Accountability Office states: The OIG's management's decision to overturn the disclaimer is—in their words—''undocumented, unexplained, and unjustified by evidence in the work papers as required by professional standards.''

This is the evidentiary gap identified by the Government Accountability Office. There is no legitimate explanation for how the auditors got from point A—the disclaimer—to point B—the clean opinion. There is no crosswalk between the two poles. It is a bridge too far.

Despite mounting questions about the opinion, the IG turned a blind eye

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 bloodstained 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

the President uses the authorities he has to deter, defend, and respond to the growing number and severity of cyber attacks, we will risk not just more of the same but emboldened adversaries and terrorist organizations that will continuously pursue more severe and destructive cyber attacks.

As ADM Mike Rogers, the commander of U.S. Cyber Command, told listeners at the Aspen Security Forum a couple weeks ago, ''to date there is little price to pay for engaging in some pretty aggressive behaviors.'' According to James Clapper, the Director of National Intelligence, ''we will see a progression or expansion of that envelope until such time as we create both a substance and psychology of deterrence. And today we don't have that.''

According to the Chairman of the Joint Chiefs of Staff, General Dempsey, our military enjoys ''a significant military advantage'' in every domain except for one—cyber space. As General Dempsey said, cyber ''is a level playing field. And that makes this chairman very uncomfortable.'' Efforts are currently underway to begin addressing some of our strategic shortfalls in cyber space, including the training of a 6,200-person cyber force. However, these efforts will be meaningless unless we make the tough policy decisions to establish meaningful cyber deterrence. The President must take steps now to demonstrate to our adversaries that the United States takes cyber attacks seriously and is prepared to respond.

This legislation before us is one piece of that overall deterrent strategy, and it is long past time that Congress move forward on information sharing legislation. The voluntary information sharing framework in this legislation is critical to addressing these threats and ensuring that the mechanisms are in place to identify those responsible for costly and crippling cyber attacks and, ultimately, deter future attacks.

Many of us have spent countless hours crafting and debating cyber legislation back to 2012. Mr. President, 2012 was the last time we attempted to pass major cyber legislation. This body has come a long way since that time. We understand that we cannot improve our cyber posture by shackling the private sector, which operates the majority of our country's critical infrastructure, with government mandates. As I argued at that time, heavyhanded regulations and government bureaucracy will do more harm than good in cyber space. The voluntary framework in this legislation represents the progress we have made in defining the role of the private sector and the role of the government in sharing threat information, defending networks, and deterring cyber attacks.

This legislation also complements actions we have taken in the National Defense Authorization Act, or NDAA, currently in conference with the House. As chairman of the Armed Services Committee, cyber security is one of my top priorities. That is why the NDAA includes a number of critical cyber provisions designed to ensure 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 NDAA 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 United States person by a foreign power. The NDAA also authorizes $200 million for the Secretary of Defense to assess the cyber vulnerabilities of every major DOD weapons system. Finally, Congress required the President to submit an integrated policy to deter adversaries in cyber space in the fiscal year 2014 NDAA. We are still waiting on that policy, and this year's NDAA includes funding restrictions that will remain in place until it is delivered.

Every day that goes by, I fear our Nation grows more vulnerable, our privacy and security are at greater risk, and our adversaries are further emboldened. These are the stakes, and that is why it is essential that we come together and pass the Cybersecurity Information Sharing Act.

Mr. President, I thank again my friend from Florida, who is a valued member of the Senate Armed Services Committee, for his indulgence to allow me to speak. I thank my colleague.

I yield the floor.

The PRESIDING OFFICER. The Senator from Florida.

NUCLEAR AGREEMENT WITH IRAN

Mr. NELSON. Mr. President, I rise to announce my decision on the Iranian nuclear agreement, the Joint Comprehensive Plan of Action.

This decision of mine comes after considerable study of the issue—as have our colleagues in the Senate taken this quite seriously. I have talked with folks on all sides of the issue. These include colleagues as well as constituents. It includes experts on the Middle East and Central Asia, arms control experts, foreign allies, and, as we say in my constituency, it includes just plain folks. I want to say that Secretary Moniz, a nuclear physicist, has been especially helpful.

Needless to say, I wish that the three Americans jailed in Iran and Bob Levinson, a former FBI agent missing in Iran for 8 years, had been a part of an agreement—of this agreement—to return them. The Levinson family in Florida is anxious for information and help to return Bob. This is personal for me.

I am a strong supporter of Israel, and I recognize that country as one of America's most important allies. I am committed to the protection of Israel as the best and right foreign policy for the United States and our allies.

I am blessed to represent Florida, which also has among our citizens a strong and vibrant Jewish community, including many Holocaust survivors and Holocaust victims' families, some of whom I have worked with to help them get just compensation from European insurance companies that turned their backs on them after World War II and would not honor their insurance claims.

In our State we are also proud to have a Floridian, a former U.S. and Miami Beach resident, as the Israeli Ambassador to the United States. Ambassador Ron Dermer grew up in Miami Beach. His father and brother are former mayors. He is someone I have enjoyed getting to know and have had several conversations with over the years and recently spent time talking to him about his opposition to this joint agreement.

I acknowledge that this has been one of the most important preparations and will be one of the most important votes that I will cast in the Senate because the foreign and defense policy consequences are both huge for the United States and our allies.

Unless there is an unexpected change in the conditions and facts before the vote is called in September—and it will be called on the very first day that we return in September—unless there is an unexpected change, I will support the nuclear agreement between Iran and the P5+1—which are the United States, the UK, France, Russia, China, and Germany—because I am convinced it will stop Iran from developing a nuclear weapon for at least the next 10 to 15 years. No other available alternative accomplishes this vital objective.

The goal of this almost 2-year negotiation—culminated in this deal—was to deny Iran from obtaining a nuclear weapon. This objective has been fulfilled in the short term. For the next 10 years, Iran will reduce its centrifuges—the machines that enrich the uranium—by two-thirds. They will go from more than 19,000 centrifuges to 6,000. Only 5,000 of those will be operating, all at Natanz, all the most basic models. The deeply buried Fordow facility will be converted to a research lab. No enrichment can occur there, and no fissile material can be stored there. For the next 15 years, Iran's stockpile of low-enriched uranium—which currently amounts to 12,000 kilograms; enough for 10 bombs—will be reduced by 98 percent, to only 300 kilograms. Research and development into advanced centrifuges will also be limited. Taken together, these constraints will lengthen the time it would take for Iran to produce the highly enriched uranium for one bomb—the so-called breakout time. It will lengthen it from 2 to 3 months that they could break out now to more than 1 year. That is more than enough time to detect and, if necessary, stop Iran from racing to a bomb.

Iran's ability to produce a bomb using plutonium will also be blocked under this deal. The Arak reactor—which as currently constructed could produce enough plutonium for one to

two bombs every year—will be redesigned to produce no weapons-grade plutonium. And Iran will have to ship out the spent fuel from the reactor forever.

Iran signed the Nuclear Non-Proliferation Treaty in 1968, in which they agreed they would not pursue nuclear weapons. Iran has reaffirmed this principle in this joint agreement. Iran also says they want to eventually make low-grade nuclear fuel, as other NPT-compliant nations do, in order to produce electricity. If they comply, they will eventually be allowed to do so under this joint agreement. Our expectation is that in 15 years, when Iran can lift the limit of 300 kilograms of low-enriched uranium, if they have not cheated, they will continue to abide by their NPT obligations and use their fuel only for electricity and medical isotopes. If they deviate from those civilian purposes, then harsh economic sanctions will result, and, very possibly, U.S. military action.

The world will be a very different place in 10 to 15 years. If we can buy this much time, instead of Iran developing a nuclear bomb in the near future, then that is reason enough for me to vote to uphold this agreement. If the United States walks away from this multinational agreement, then I believe we would find ourselves alone in the world with little credibility, but there are many more reasons to support this agreement.

The opponents of the agreement say that war is not the only alternative to the agreement. Indeed, they, as articulated by the Israeli Ambassador, say we should oppose the agreement by refusing to lift congressional economic sanctions, and the result will be that the international sanctions will stay in place, that Iran will continue to feel the economic pinch, and therefore Iran will come back to the table and negotiate terms more favorable to the United States and our allies.

If the United States kills the deal that most of the rest of the world is for, there is no question in this Senator's mind that the sanctions will start to erode, and they may collapse altogether. We just had a meeting with all the P5+1 Ambassadors to the United States, and they reaffirmed that exact fact. Sanctions rely on more than just the power of the U.S. economy, they depend on an underlying political consensus in support of a common objective. China, Russia, and many other nations eager to do business with Iran went along with our economic sanctions because they believed they were a temporary cost to pay until Iran agreed to a deal to limit their nuclear program. That fragile consensus in support of U.S. policy is likely to fall apart if we jettison this deal.

I think it is unrealistic to think we can stop oil-hungry countries in Asia from buying Iranian oil, especially when offered bargain basement prices. It is equally unrealistic to think we can continue to force foreign banks that hold the Iranian oil dollars—banks in China, India, Japan, South Korea, and Taiwan that have sequestered Iranians' oil dollars—it is unrealistic to expect that they will hold on to that cash simply because we threaten them with U.S. banking sanctions. How will such threats be taken seriously when these countries, taken together, hold nearly half of America's debt, making any decision to sanction them extraordinarily difficult. Killing this deal by rejecting it means the sanctions are going to be weaker than they are today, not stronger, and the United States cannot simply get a better deal with Iran, with less economic leverage and less international support. That is a fact we are having to face. Of course, if we rejected it and if the sanctions crumbled, all of this would probably happen while Iran would be racing to build a bomb. Without this deal, Iran's breakout time could quickly shrink from months to a handful of weeks or days.

It is reasonable to ask why Iran would agree to negotiate a delay in their nuclear program that they have advanced over the years at the cost of billions of dollars. The simple answer is they need the money. The Iranian economy is hurting because of the sanctions, and Iran's Supreme Leader needs to satisfy rising expectations of average Iranians, who are restless to have a bigger slice of the economic pie with more and better goods and supplies.

So they have an interest in striking a deal, but does that mean we trust Iran's Government? No, not at all. The Iranian religious leadership encourages hardliners there to chant ''Death to America'' and ''Death to Israel.'' Therefore, this agreement can't be built on trust. We must have a good enough mechanism in place to catch them when and if they cheat; in other words, don't trust but verify.

I believe the agreement sets out a reasonable assurance that Iran will not be able to hide the development of a bomb at declared or undeclared sites. The International Atomic Energy Agency inspectors will have immediate access to declared sites—the Arak reactor and the enrichment facilities at Natanz and Fordow.

For the next 20 to 25 years, inspectors will also have regular access to the entire supply chain, including uranium mines and mills, centrifuge production, assembly, and storage sites. That means inspectors will catch Iran if they try to use the facilities we know about to build a weapon or if they try to divert materials to a secret program. To confirm that Iran is not building a covert bomb, this agreement ensures that inspectors will have access to suspicious sites with no more than a 24-day delay. I know there has been a lot of conversation about that. It is broken off into days. At the end of the day, it must be physical access. Now, would this Senator prefer they get in instantaneously? Of course. Could Iran hide some activities relevant to nuclear weapons research? Possibly. But to actually make a bomb, Iran's secret activity would have to enrich the fuel for a device—and they couldn't cover that up if they had years, let alone do so in a few weeks. Traces of enriched uranium or a secret plutonium program do not suddenly vanish, and they can't be covered up with a little paint and asphalt. So I am convinced that under the agreement, Iran cannot cheat and expect to get away with it.

On top of the unprecedented IAEA inspections established by this deal is the vast and little understood world of American and allied intelligence. This Senator served on the Intelligence Committee for 6 years and now has clearances on the Armed Services Committee. I can state unequivocally that U.S. intelligence is very good and extensive and will overlay IAEA inspections. Remember, we discovered their secret activities in the past, even without the kinds of inspections put in place by this joint agreement. So if Iran tries to violate its commitment—its commitment not to build nuclear weapons—and if the IAEA doesn't find out, I am confident our intelligence apparatus will.

What about the part of the joint agreement that allows the conventional arms embargo to be lifted in 5 years and missile technology to be lifted in 8 years? I understand it was always going to be tough to keep these restrictions in place, and I don't like that those restrictions are not there. Fortunately, even when the arms embargo expires, five other U.N. resolutions passed since 2004 will continue to be in force to prohibit Iran from exporting arms to terrorists and to militants. These have had some success, albeit limited, as in the case of the U.S. Navy stopping arms shipments to the Houthis in Yemen. These same U.N. resolutions will stay in place to block future Iranian arms shipments to others. We also have nonnuclear sanctions tools we can—and we must—continue to use to go after those who traffic in Iranian arms and missiles.

Will this agreement allow Iran to continue to be a state sponsor of terrorism? Yes, but they now have the capability to develop a nuclear weapon within months and still be a state sponsor of terrorism. I believe it is in the U.S. interest that Iran is not a nuclear power sponsoring terrorism. As dangerous a threat that Iran is to Israel and our allies, it would pale in comparison to the threat posed to them and to us by a nuclear-armed Iran.

Would I prefer a deal that dismantles their entire program forever and ends all of Iran's bad behavior? Of course I would. But how do we get a better deal that the opposition wants? We don't have that opportunity if the sanctions fall apart, and that is exactly what would happen if we reject this deal. Iran will emerge less isolated and less constrained to build a nuclear weapon.

Under the deal, we keep most of the world with us. That means, if the Iranians cheat, they know we can snap back the economic sanctions and cut off their oil money. This joint agreement declares that Iran will never ever be allowed to develop a nuclear weapon. If they break their agreement, even in 10 or 15 years, every financial and military option will still be available to us, and those options will be backed by ever-improving military capabilities and more and better intelligence.

So when I look at all the things for the agreement and against the agreement, it becomes pretty obvious to me to vote in favor of the agreement.

I yield the floor.

The PRESIDING OFFICER. The majority leader.

Mr. MCCONNELL. Mr. President, our government was recently struck by a devastating cyber attack that has been described as one of the worst breaches in U.S. history. It was a major blow to the privacy of millions of Americans. We know the private sector is vulnerable to attack as well. The House has already passed two White House-backed cyber security bills to help address the issue. Similar legislation is now before the Senate. It is strong, bipartisan, and transparent. It has been vetted and overwhelmingly endorsed 14 to 1 by both parties in committee.

It would help both the public and private sectors to defeat cyber attacks. The top Senate Democrat on this issue reminds us it would protect individual privacy and civil liberties too. Now is the time to allow the Senate to debate and then pass this bipartisan bill.

In just a moment, I will offer a fair consent request to allow the Senate to do just that. The Democratic leader previously said that both he and the senior Senator from Oregon believe the Senate should be able to finish the bill ''in a couple of days . . . at the most.'' And just today he said the Democrats remain willing to proceed to this bipartisan bill if allowed to offer some relevant amendments. The senior Senator from New York has also said that Democrats want to get to the bill and that they want to get a few amendments too.

Our friends across the aisle will be glad to know that the UC I am about to offer would allow 10 relevant amendments per side to be offered and made pending. That is a good and fair start that exceeds the request from our friends across the aisle.

Now that we have a path forward that gives both sides what they said they need, I would invite our colleagues to join us now in moving forward on this bill. I invite our colleagues to allow the Senate to cooperate in a spirit of good faith to pass a bill this week so we can help protect the American people from more devastating cyber attacks.

I notified the Democratic leader that I would propound the following consent request: I ask unanimous consent that the cloture motion on the motion to proceed to calendar No. 28, S. 754, be withdrawn and that the Senate immediately proceed to its consideration. I further ask that Senator BURR then be recognized to offer the Burr-Feinstein substitute amendment and that it be in order during today's session of the Senate for the bill managers, or their designees, to offer up to 10 first-degree amendments relevant to the substitute per side.

The PRESIDING OFFICER. Is there objection?

Mr. REID. Reserving the right to object.

The PRESIDING OFFICER. The minority leader.

Mr. REID. The Republican leader is my friend, and I don't mean in any way to disparage him, other than to bring out a little bit of history. I can't imagine how he can make this offer with a straight face. Have amendments pending? That is like nothing. We tried that before, as recently as the highway bill. Having amendments pending doesn't mean anything.

We want to pass a good cyber security bill. We have a bill that has been crafted in the intelligence committee. Other committees have been interested in participating in what we have here on the floor, but they are willing to say: OK. We have a bill from the intelligence committee.

There have been no public committee hearings, no public markups. There has been nothing done other than a rule XIV which, of course, my friend said he would not do if he got to be the leader and there would be a robust amendment process. Having a robust amendment process has nothing to do with having amendments pending.

We want to pass a good bill. But we want to have a reasonable number of amendments, and there will be votes on those amendments. We are not asking for longtime agreements. The Republican leader's proposal would not lead to votes on the amendments. He would allow the amendments to be pending, but if the Republican leader were to file cloture, as he has done repeatedly the last few months—and an example is what he did with the recent highway bill—all amendments that were not strictly germane would fall.

Remember, we are not asking for germane amendments. We are asking for relevant amendments. We are willing to enter into an agreement that provides votes on a reasonable number of amendments that would be germane in nature, and we should be working on that agreement.

In contrast, if we fail to get that agreement, we are going to have a cloture vote an hour after we come in in the morning, and 30 hours after that—sometime late Thursday afternoon or early Thursday evening—he would have to file cloture on that. That puts us right into the work period when we get back on September 8.

When we get back, we have the 8th to the 17th, including weekends and a holiday that is celebrated every year that we always take off, which includes 2 days. It is a Jewish holiday. I can't imagine why we would want this to interfere with what we are trying to do in the month of September.

We are willing to do this bill. We can start working on these amendments right now if we can have votes on them, but we are not going to agree to some arrangement like this. If the Republicans are going to push this, we can come in here tomorrow, and we will vote. The 30 hours of time will go by—and we know how to use 30 hours; we were taught how to do that—30 hours of postcloture time. And Thursday afternoon, the leader can make whatever decision is necessary.

We want a cyber bill. This bill is not the phoenix of all cyber bills, but it certainly is better than nothing. We should—following the recommendation and the suggestion and what the Republican leader has said he would do—be allowed some amendments to vote on. We can start that today. Today is Tuesday. We can finish these amendments—I would hope on the Democratic side—in a fairly short order of time.

As for the Republicans, I don't know. All I heard following the caucus is one Republican Senator wanted to offer an amendment on the cyber bill dealing with auditing the Fed. I can't imagine why that has anything to do with this bill.

We are serious about legislating. We want to do something that is good, we believe, for the country, good for the order of the Senate. Otherwise, we will look at each other around here until Thursday afternoon, and the Republican leader can look forward to this being the first thing we take up when we get back in September. We are willing to be fair and reasonable to finish this, with our amendments, in a very short period of time. So I object.

The PRESIDING OFFICER. Objection is heard.

Mr. MCCONNELL. Mr. President, let me say, I think there may well be a way forward here. What I thought I heard the Democratic leader say is that they are interested in passing a bill. That is important. He said when it was offered on the defense authorization bill that it was a 2-day bill, and we could agree to a limited number of amendments.

I think we both agree this is an important subject. I can't imagine that either the Democrats or the Republicans want to leave here for a month and not pass the cyber security bill. I think there is enough interest on both sides to try to continue to discuss the matter and see if there is a way forward. That would be in the best interest of the country if we could come together and do this. This bill came out of the intelligence committee 14 to 1.

Chairman BURR and Vice Chair FEINSTEIN have been asking for floor time. They are anxious to move this bill

across the floor. I am hoping the Democratic leader and I can continue to discuss the matter and that we can find a way forward.

The PRESIDING OFFICER. The Democratic leader.

Mr. REID. Mr. President, I look forward to that discussion. Keep in mind, being reported out of committee—this is a committee that holds everything in secret. They do nothing public. So having a 14 to 1 vote in a meeting that takes place in secret doesn't give the other Senators who are not on that committee a lot of solace.

I look forward to the Republican leader and me and our staffs working together to try to come up with some way to move forward on this legislation. We want to do that.

The PRESIDING OFFICER. The majority leader.

Mr. MCCONNELL. Mr. President, as my good friend the Democratic leader used to remind me, the majority leader always gets the last word.

This is not a new issue. It was around during the previous Congress. Other committees acted—other committee chairmen like what Chairman BURR and Vice Chair FEINSTEIN have done. Hopefully, we can minimize sort of manufacturing problems here that keep us from going forward when it appears to me that both sides really would like to get an outcome and believe it would be best for the country to get an outcome before we go into the recess. We will continue to discuss the matter and hope that we can find a way forward.

The PRESIDING OFFICER (Mr. LANKFORD). The Senator from Oregon.

Mr. WYDEN. Mr. President, I will be very brief. I understand there has already been an objection.

I will speak later in the afternoon or early evening in some detail about why I have significant reservations with respect to this legislation.

To say—as we heard again and again throughout the day—that this is about voluntary information sharing is essentially only half true. The fact is, companies could volunteer to share their customers' information with the government, but they wouldn't have to ask for permission from their customers before handing it over. That is one reason every major organization with expertise and interest on privacy issues has had reservations about the bill. It may be voluntary for companies, but it is mandatory for their customers and their consumers. They are not given the opportunity to opt out.

The legislation has been public for months, and dozens of cyber security experts have said it wouldn't do much to stop sophisticated, large-scale attacks such as the horrendous attack at the Office of Personnel Management.

On Friday, the Department of Homeland Security—an absolutely essential agency as it relates to this bill—wrote a letter to our colleague, the distinguished Senator from Minnesota, Mr. FRANKEN, and said if this bill's approach is adopted, ''the complexity and inefficiency of any information sharing program will markedly increase.'' The Department of Homeland Security added that the bill ''could sweep away important privacy protections.'' That is a pretty strong indictment from the agency that would be in charge of implementing the legislation.

As I have indicated a couple of times in the last day or so, I think the managers, Senator FEINSTEIN and Senator BURR, have made several positive changes, but the bottom line is it doesn't address the very substantial privacy concerns that relate to this bill. The fact is, cyber security is a very serious problem in America.

Oregonians know a lot about it because one of our large employers was hacked by the Chinese. SolarWorld was hacked by the Chinese because they insisted on enforcing their rights under trade law. In fact, our government indicted the Chinese for the hack of my constituents and others.

So cyber security is a serious problem. Information sharing can play a constructive role, but information sharing without robust privacy safeguards is really not a cyber security bill. It is going to be seen by millions of Americans as a surveillance bill, and that is why it is so important that there be strong privacy guidelines.

The fact is, in the managers' legislation, the section allowing companies to hand over large volumes of information with only a cursory review would be essentially unmodified. The Department of Homeland Security asked for some specific changes to the language, which the managers' amendment does not include. So my hope is, we are going to have a chance to have a real debate on this issue. Personally, I would rather go down a different route with respect to cyber security legislation. In particular, I recommend the very fine data breach bill of our colleague from Vermont Senator LEAHY, but if Senators have their hearts set on doing the bill before us, it is going to need some very substantial amendments, both to ensure that we show the American people that security and privacy are not mutually exclusive, that we can do both, and to address the very serious operational reservations the Department of Homeland Security has raised. Neither set of concerns is thoroughly addressed by the managers' amendment.

So my hope is that we are going to have a chance to make some very significant reforms in this legislation. After seeing what has happened over the last few weeks, where the government isn't exactly doing an ideal job of securing the data it has, and now we are going to propose legislation that has private companies, without the permission of their customers, for example, to dump large quantities of their customers' data over to the government with only a cursory review—this legislation is not going to be real attractive to the millions of Americans who sent us to represent them.

In fact, in just the last few days, I read in the media that some of the opponents of this legislation have sent something like 6 million faxes to the Senate—and people wonder if there are still fax machines. I guess the point is to demonstrate it is important that we understand, as we look at digital communications, what the challenge is.

I will have more to say about this later in the afternoon and in the evening, but I wanted to take this opportunity, since we have just gotten out of the party caucuses, to make some corrections with respect to what we were told this morning and particularly on this question about how this is a voluntary bill. Ask millions of Americans whether it is voluntary when companies can hand over their private information to the government without their permission.

I yield the floor.

The PRESIDING OFFICER. The Senator from Kansas.

Mr. MORAN. Mr. President, I ask unanimous consent to be recognized as in morning business.

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

NUCLEAR AGREEMENT WITH IRAN

Mr. MORAN. Mr. President, cyber security is an important issue, but I come to the floor to talk for a bit about one of the most consequential decisions that I, as a Member of the U.S. Senate, and my colleagues will make, and that concerns the negotiated agreement between the P5+1 and Iran—the proposed Joint Comprehensive Plan of Action with Iran. In my view, it provides too much relief in return for too few concessions. The deal implicitly concedes that Iran will become a nuclear power and will gain the ability and legitimacy to produce a weapon in a matter of years while gaining wealth and power in the meantime.

I serve on the Senate Banking Committee. The sanctions that were created by Congress originate from that committee. Those sanctions were put in place to prevent Iran from becoming a nuclear power—a country capable of delivering a nuclear weapon across their border. Those sanctions were not put in place to give Iran a path or a guideline to become a nuclear-weapon-capable country. The key is to keep nuclear weapons out of the hands of Iran's Government. The key to that is to permanently disable Iran from nuclear capability and remove the technology used to produce nuclear materials. This deal fails to achieve this goal by allowing Iran to retain nuclear facilities. Though some of it will be limited in use in the near term, the centrifuges used to enrich nuclear matter will not be destroyed or removed from the country. This deal allows Iran's nuclear infrastructure to remain on standby for nuclear development when the restrictions expire.

Also troubling is the agreement's lack of restrictions on nuclear research and development. Iran seeks to replace its current enrichment technology

with a more advanced centrifuge that more efficiently enriches nuclear material. By failing to restrict research and development now, we are priming Iran's nuclear program to hit the ground running toward a bomb once the restrictions are lifted in a matter of years.

Also, the inspection regime agreed to in this negotiation is dangerously accommodating. The agreement provides Iran a great deal of flexibility regarding the inspection of military sites just like those where Iran's past covert nuclear development work took place. The deal allows Iran to hold concerned international inspectors at bay for weeks, if not months, before granting access to a location suspected of being a site for nuclear development.

The value of any access to suspected Iranian nuclear sites that international inspectors ultimately do receive will depend upon their understanding of Iran's past nuclear weapons research. A comprehensive disclosure of possible military dimensions to Iran's nuclear research is necessary for inspectors to fully understand Iran's current infrastructure and is critical to their ability to rule out any future efforts to produce nuclear weapons.

The International Atomic Energy Agency, IAEA, has not made public its site agreement with Iran about their previous nuclear developments. This is an aside, but I would say none of us should agree to this negotiated agreement without seeing, reading, and knowing the content of that agreement. Under the proposed deal, that vital full disclosure of Iran's nuclear past may not occur, diminishing the value of inspections and increasing the risk that another covert weaponization of Iran will take place.

Painfully absent from the agreement's requirements is Iran's release of American hostages: Saeed Abedini, Jason Rezaian, Robert Levinson, and Amir Hekmati. The freedom of Americans unjustly held in Iran should have been a strict precondition for sanctions relief instead of an afterthought.

In return for very limited concessions, this deal gives Iran way too much. If implemented, the agreement would give Iran near complete sanctions relief up front. This isn't a Republican or Democratic issue. Common sense tells us that you don't give away a leverage until you get the result that you are looking for, and this agreement provides sanctions relief upfront, delivering billions in frozen assets to the Iranian Government and boosting the Iranian economy. Included in this relief are sanctions related to Iran's Revolutionary Guard Corps, which were to be lifted only when Iran ceased providing support for international terrorism.

The sanctions relief in this proposal not only fails to require preconditions and cooperation regarding nuclear disarmament but will remove sanctions from the Iranian Guard, despite their status as a top supporter of terrorist groups around the Middle East and globe.

This type of gratuitous flexibility for Iran is found elsewhere in the agreement. The P5+1 acceptance of Iranian demands for a relaxed U.N. arms embargo is both perplexing and scary. This deal would relax trade restrictions on missiles after 8 years, while immediately erasing limits on missile research and development. It would also lift restrictions on Iranian centrifuge use and development after just 8 to 10 years. The deal grants Iran the ability to more efficiently produce nuclear material just as it gains the ability to access the delivery weapons system.

Earlier this month, the Chairman of the Joint Chiefs of Staff, GEN Martin Dempsey, said: ''Under no circumstances should we relieve pressure on Iran relative to ballistic missile capabilities and arms trafficking.'' Lifting the U.N. arms embargo was ''out of the question.'' Yet, just 1 week later, negotiators announced the lifting of the embargo in 5 to 8 years or less. I wonder what has changed. Unless the menace of an increased flow of weapons in and out of Iran somehow substantially decreased during the intervening week, the consequence of this sudden capitulation should have us all greatly concerned.

This fear of increased money flow to terror organizations linked to the Iranian Government is not based upon merely an outside possibility; it is a likelihood. Last week Iran's Deputy Foreign Minister stated: ''Whenever it's needed to send arms to our allies in the region, we will do so.'' More money and more weapons in the hands of terrorist organizations are the fuel for increased violence and further destabilization in the conflict-torn Middle East.

We have little reason to believe Iran's behavior will change as a result of this agreement. In fact, their chants of ''Death to America'' become more real.

Since the announcement of the agreement, the leader of Iran has been openly antagonistic to the United States. Ayatollah Ali Khamenei has promised to continue to incite unrest and said Iran's ''policy towards the arrogant U.S. will not change.'' These anti-American statements come from an Iranian leader whose commitment the Obama administration is relying on for the nuclear accord to work. It should trouble every American that the Obama administration is asking us to support a deal that relies on the total cooperation of those who, as I say, strongly state their commitment to bringing about ''death to America.''

Given the Obama administration's troubling efforts to push through this deal to the United Nations and restrict the influence of the American people through this Congress in the decision, it is all the more important that we follow through with a serious assessment of this nuclear agreement. We are faced with a circumstance that, by the administration's own previous standards, concedes too much and secures too little.

I strongly oppose this nuclear deal. It is intolerably risky, and the result will be a new Iran—a legitimized nuclear power with a growing economy and enhanced means to finance terror, to antagonize, and to ultimately pursue a nuclear weapons program. I will support the congressional resolution to express Congress's explicit disapproval.

President Obama has used fear in his agenda in seeking our support for this agreement. The warning has been that a vote against his policy is a vote for war with Iran. The President's political scare tactics are not only untrue but also illogical.

Incidentally, we were not at war with Iran when the agreements were in place before the negotiation. The absence of agreeing to the negotiated agreement would not mean we will be at war thereafter.

The President's claims undermine numerous statements his own administration has made about the negotiation process, the nature of the Iranian nuclear program, and the proposed agreement's prospects for success. If true, the President's words concede that his foreign policy has led America into a dangerous position.

We would expect a President to provide the American people as many alternatives to war as possible, not just a single narrow and risky one such as this. According to the President, the only alternative to war is this agreement—a deal that results in better financed terrorists, a weakened arms embargo, and the need for boosting U.S. weapons sales to Iran's regional rivals. If this prospect of war is his concern, the President would benefit by reevaluating the geopolitical consequences of the deal and seeking out much better options.

I had hoped these negotiations would result in a strong but fair deal to dismantle Iran's nuclear infrastructure. Again, the purpose of placing sanctions on Iran was to get rid of their nuclear capability as far as delivery of nuclear material across their borders. Yet this agreement leaves that infrastructure in place and puts them on a promising path toward that nuclear capability.

Regrettably, that kind of deal was not reached. Now my hope is a simple one: that we are able to reverse some of the damage that is already done and that this agreement is rejected.

I would say that there are those who argue that we would be isolated by rejection of this agreement, that other countries would approve and the United Nations may approve. This is an issue of such importance that we need to do everything possible to see that Iran does not become a nuclear power, and we need to have the moral character and fiber to say no to this agreement.

Mr. President, I yield the floor.

The PRESIDING OFFICER. The Senator from Washington.

Mrs. MURRAY. Mr. President, I ask unanimous consent to speak as in morning business.

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

ECONOMIC SECURITY FOR OUR COUNTRY'S WORKERS

Mrs. MURRAY. Mr. President, across our country today, so many of our workers clock in 40 hours a week. They work very hard, and yet they are unable to provide for their families.

Just last fall, NBC News interviewed a woman named Latoya who worked in a fast food restaurant. She was protesting as part of a fast food workers strike. Latoya is raising four children alone on $7.25 an hour. That is less than $300 a week and is well below the poverty line for her and her family. For part of last year, she was living in a homeless shelter. She told the reporter: ''Nobody should work 40 hours a week and find themselves homeless.'' On top of rock-bottom wages, Latoya said she and her colleagues experienced unpaid wages, unpredictable scheduling, and having to make do with broken equipment on the job.

In today's economy, too many of our workers across the country face the same challenges as Latoya. They are underpaid, they are overworked, and they are treated unfairly on the job. In short, they lack fundamental economic security.

Several places around the country and in my home State of Washington are working to address this at the local level. This Senator believes we need to bring the Washington State way here to Washington, DC. In Congress, I believe we need to act to give workers some much needed relief. We need to grow our economy from the middle out, not the top down, and we should make sure our country works for all Americans, not just the wealthiest few.

There is no reason we can't get to work today on legislation to do just that. That is why I have joined with my colleagues over the past few months in introducing several bills that will help restore some much needed economic security and stability to millions of workers. That is why I am hoping we can move some of these bills forward before we all go back home to our States.

For too long we have heard from some Republicans the theory—a deeply flawed theory—that if we would only grant more tax cuts to the wealthiest Americans and if we would just keep rolling back regulations on the biggest corporations, those benefits would eventually trickle down and reach working families in our country. Not only does that theory not work, as we have seen over the past few decades, that trickle-down system has done real damage to our Nation's middle class and our working families. While worker productivity has actually reached new heights, workers have lost basic protections they once had.

While trickle-down economics allows corporations to post big profits, too many of our workers are paying the price. Let me give some examples. Today the Federal minimum wage can leave a family in poverty even after working full time and even without taking a single day off. Not only that, today some businesses are using unfair scheduling practices to keep workers guessing about when they are going to be called in to work, with no guarantee of how much money they will earn in a given week. Those types of scheduling abuses take a real toll on workers' lives and prevent them from getting ahead. Attending college classes is not an option when someone's work schedule is always in flux. Taking on a second job to earn more money is nearly impossible when you can't plan around your first job. And that is not all. Today, 43 million workers in this country don't have paid sick leave. When they get sick, they have to choose between toughing it out at work and passing that illness on to others or staying at home and potentially losing their job. When their child is sick, they have to choose between losing money on their paycheck or missing out on caring for their son or daughter. If that is not enough, in our country women are paid just 78 cents for every dollar a man makes. That is not just unfair to women, by the way; it is bad for families and it hurts our economy.

Many businesses are doing the right thing and are supporting their workers, but other corporations that don't, put those businesses that are doing the right thing at a competitive disadvantage by running a race to the bottom and pulling their workers down with them.

This worker insecurity isn't just devastating for the millions of workers and their families who are impacted by it, it is also hurting our economy. Truly robust and strong economic growth comes from the middle out, not the top down. When our workers lack security, when they are not treated fairly, they can't invest in themselves and their children or spend money in their communities or move their families into a middle-class life.

I believe we have to address this challenge on multiple fronts. We can start by making sure our workers are treated fairly so they can earn their way toward rising wages and increased economic security.

There are important things we can do here in Congress to expand economic security and stability for millions of our working families today. For starters, we should pass the Paycheck Fairness Act that the senior Senator from Maryland has championed for so many years to finally close the pay gap between men and women. The Paycheck Fairness Act would tackle pay discrimination head-on. This Senator hopes we can all agree that in the 21st century, workers should be paid fairly for the work they do, regardless of their gender.

We should also raise the minimum wage to make sure hard work does pay off. My Raise the Wage Act increases the minimum wage to $12 by 2020 and is enough to lift a family of three out of poverty. It will put more money in workers' pockets so they can spend it in their local communities. It will help to build a strong floor—a Federal minimum—that workers and cities can build off of and go even higher where it makes sense, like in Seattle in my home State in Washington. It is a level that Republicans should be able to agree with and start moving toward right now.

I have also worked on a bill, along with Senators WARREN and MURPHY, to crack down on the scheduling abuses I just talked about, so businesses would no longer keep their workers guessing on when they would be called in or how many hours they might get in a given week.

In February I introduced the Healthy Families Act to allow workers to earn up to 7 paid sick days. I want to move forward on that legislation to give our workers some much needed economic security because no one should have to sacrifice a day of pay or their job altogether just to take care of themselves or their sick child.

We as a nation should not turn our backs on empowering our workers through collective bargaining, especially since strong unions ensure workers have a strong voice at the table. It is the very thing that helped so many workers climb into the middle class in this country.

Enacting these critical policies won't solve every problem facing our workers and their families today. It is not the only way that I and Senate Democrats will be fighting to protect workers and making sure the economy is growing from the middle out, not the top down. But these policies would be very strong steps in the right direction to bring back that American dream of economic security and a stable middle-class life for millions of workers who have seen it slip away.

When workers succeed, businesses succeed and thus the economy succeeds. We know this works. I have seen it in my home State of Washington where State and local governments have taken the lead on proposals such as raising the minimum wage and paid sick days. I think it is time to bring some of that Washington State way right here to Washington, DC.

I recently heard from a small business owner by the name of Laura. She owns a small auto repair shop in Renton, WA. She shared something that I hear all the time from business owners: Doing the right thing by workers starts a virtuous cycle. Laura said, ''When workers have more money, businesses have more customers. With more customers, businesses can hire more workers, which in turn generates more customers.''

Working families in our country have been waiting long enough for some relief from the trickle-down system that hurts the middle class. That is why I

am going to be asking for unanimous consent to work on the policies that would restore economic security and stability to more workers.

Let's finally restore some stability and security for workers across our country. Let's make sure hard work pays off. Let's help more families make ends meet, expand economic opportunity, and grow our economy from the middle out.

Thank you, Mr. President.

I yield the floor.

The PRESIDING OFFICER. The Senator from Arizona.

Mr. MCCAIN. Mr. President, I ask unanimous consent that I be allowed to speak for 3 minutes and that I be followed immediately by the Senator from Idaho.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

Mr. MCCAIN. Mr. President, is the parliamentary procedure that there was an objection to the Senate moving forward with the consideration of the cyber bill? Is that correct?

The PRESIDING OFFICER. There was an objection that was heard to the request of the majority leader.

Mrs. MURRAY addressed the Chair.

Mr. MCCAIN. Mr. President, do I have the floor?

The PRESIDING OFFICER. The Senator from Arizona has the floor.

Mr. MCCAIN. I have the floor, I tell the Senator from Washington.

This is unbelievable. It is unbelievable that this body would not move forward with a cyber bill with the situation of dire consequences and dire threats to the United States of America. Admiral Rogers, the commander of U.S. Cyber Command, told listeners at the Aspen Security Forum that ''to date there is little price to pay for engaging in some pretty aggressive behaviors.''

According to James Clapper, the Director of National Intelligence, ''we will see a progression or expansion of that envelope until such time as we create both the substance and psychology of deterrence. And today we don't have that.''

The Chairman of the Joint Chiefs of Staff, General Dempsey, our military enjoys ''significant military advantage'' in every domain except for one—cyber space. General Dempsey said cyber ''is a level playing field. And that makes this chairman very uncomfortable.'' The Chairman of the Joint Chiefs of Staff is uncomfortable about the cyber threats to this Nation.

What just took place is millions of Americans had their privacy hacked into. God only knows what the consequences of that are. The other side has decided to object to proceeding with a bill that passed through the Intelligence Committee by a vote of 14 to 1. This is disgraceful—this is disgraceful. I tell my colleagues on the other side of the aisle, by blocking this legislation, you are putting this Nation in danger. By blocking this legislation, you are putting this Nation in danger by not allowing the Senate of the United States to act against a very real threat to our very existence.

I say this is a shameful day in the Senate. I urge the Democratic leader to come to the floor and allow us to consider amendments, move forward with this legislation because the security of the United States of America is in danger.

I thank my colleagues.

I yield the floor.

The PRESIDING OFFICER. The Senator from Idaho.

SAWTOOTH NATIONAL RECREATION AREA AND JERRY PEAK WILDERNESS ADDITIONS ACT

Mr. RISCH. Mr. President, is H.R. 1138 at the desk?

The PRESIDING OFFICER. The Senator is correct.

Mr. RISCH. Mr. President, I ask unanimous consent that the Senate proceed to the immediate consideration of H.R. 1138, which has been received from the House.

The PRESIDING OFFICER. The clerk will report the bill by title.

The bill clerk read as follows:

A bill (H.R. 1138) to establish certain wilderness areas in central Idaho and to authorize various land conveyances involving National Forest System land and Bureau of Land Management land in central Idaho, and for other purposes.

There being no objection, the Senate proceeded to consider the bill.

Mr. RISCH. Mr. President, I ask unanimous consent that the bill be read a third time and passed, the motion to reconsider be laid upon the table, and that any statements relating to the bill be printed in the RECORD.

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

The bill (H.R. 1138) was ordered to a third reading, was read the third time, and passed.

Mr. RISCH. Mr. President and fellow Senators, today is a historic day for the State of Idaho. This is the creation of a wilderness area in the Sawtooth area of Idaho, the Boulder-White Clouds area, and the Jerry Peak area. These two mountain ranges and one mountain peak area have been under consideration for about 10 years.

I want to talk very briefly about what we are dealing with. These are some of the most magnificent pieces of land, not only in Idaho but in the United States. Before anyone goes abroad to see the Champs-Elysees or to see the magnificent works of art in Italy, you need to put on your list seeing the Boulder-White Clouds area. It is truly a magnificent area.

What we just did was we created a wilderness of about 275,000 acres that creates these three wilderness areas, plus a buffer zone around them. It is a great day for Idaho. This is an Idaho solution to an issue that has been pending for some time.

I conclude by simply stating that all credit for this goes to Congressman MIKE SIMPSON. Congressman SIMPSON started working on this about 10 years ago and wanted to put together, in a collaborative fashion, a wilderness bill for this particular area. He did that. He brought it back to Washington, DC. Because of the situation in DC at the time, the bill was changed greatly and was no longer an Idaho solution to the Idaho problem.

Congressman SIMPSON did not give up. He worked and he worked and he worked at it. It is truly his long-term commitment to this and his long work on this that got us to this point. What he did was take this land that there was virtually unanimous agreement should be in wilderness; that is, the heart of this area, the Boulder Range, the White Cloud Range, and the Jerry Peaks area.

There was unanimous agreement that this is the kind of land that needs to be in wilderness. Indeed, when I was Governor, I wrote this rule for several million acres. This was included in it. It was protected as wilderness. This is not changing the character of it in that regard. What it does is put it in statute instead of in rule.

The difficulty was, as always with these kinds of areas, the buffer area around what everybody agrees is truly unique ground that should be handled as wilderness. Obviously, it is an area that ingrains passion in people. It causes people to have strong feelings about the area. As a result of that, people fight to protect what they think should be protected, and just as much, people who use the buffer zones for different reasons feel just as passionately the other way.

What Congressman SIMPSON was able to do was get everybody to the table in a very collaborative fashion, to where he got the wilderness preservationists, the hikers, the backpackers, the horse people, the motorized users, including snowmobile, ATV, and motorcycle people, to all agree to a management plan for everything that is included in this bill.

Congressman SIMPSON was tenacious on this. He gets the full credit for this. I think Idahoans will truly appreciate this for many years. There is no doubt in my mind that the efforts Congressman SIMPSON put into this will be greatly appreciated for years and years to come.

With that, I yield the remainder of my time to my colleague, my good friend, Senator MIKE CRAPO.

The PRESIDING OFFICER. The Senator from Idaho.

Mr. CRAPO. I thank Senator RISCH.

Mr. President, it is an honor for me to rise with my colleague JIM RISCH to celebrate the passage of this legislation. It has been years and years in the making. This legislation culminates from the hard work by people all over Idaho. As Senator RISCH has indicated, the credit for making this all finally come together goes to Representative MIKE SIMPSON. I wholeheartedly agree with that.

Passage of the Sawtooth National Recreation Area and Jerry Peak Wilderness Additions Act, also called the SNRA+ Act, is the result of tremendous efforts by Representative SIMPSON and Senator RISCH. He deserves tremendous credit as well. I do want to say that I honor Representative SIMPSON's dogged determination and his persistence to fight through many obstacles associated with this treasured region of our State for a very long period of time.

Representative SIMPSON's efforts have given Idaho a homegrown solution to what was rapidly becoming a national problem. As I said, similarly, my colleague Senator RISCH has fought through many challenges in his pursuit of developing a consensus on this issue that has been hard to achieve. Both of my colleagues, in their respective ways, have expressed again the power of collaboration in the attempt to find consensus to deliver local solutions to longstanding public land management challenges in Idaho.

Local governments and local stakeholders must be empowered to shape and manage decisions relating to our public lands. In the process, such efforts must respect private property rights and the owners of private property as well as other impacted stakeholders. Such initiatives are never easy to achieve, and consensus takes dedication, patience, and persistence. For too long, westerners have been saddled with top-down land management decisions that are both harmful to the landscape and the people living in and subsisting off of our natural treasures. The SNRA+ is a win for Idaho and an example of how local governments and interests can achieve solutions to some of the most persistent public land management issues we face.

I have to conclude by saying that while we have succeeded today in passing a milestone in Congress, the focus must now shift to the hard work of successful implementation that will require commitment from the various Federal agencies and all of the affected interests.

Again, I commend Senator RISCH and Representative SIMPSON for their incredibly important work that has been accomplished today.

I yield the floor.

The PRESIDING OFFICER. The Senator from Nevada.

Mr. HELLER. Mr. President, I congratulate my colleagues from Idaho on this particular piece of legislation, proving it can be done right. It was just a few weeks ago that the President unilaterally declared a monument in the State of Nevada the size of Rhode Island, with two counties that had no input in the process. Our delegation had no input. The collaborative effort that we saw from Idaho and how it works and how the system should work needs to be recognized. What happened in Nevada, I feel, was a disgrace.

It is a shame we are standing here today with a monument in the State of Nevada the size of Rhode Island with no input from Nevada's delegation or counties, just a single action made by one person.

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

Mr. HELLER. Mr. President, I would like to talk about personal privacy rights for American citizens. It was just 2 months ago that the Senate took action to restore privacy rights of American citizens through the USA FREEDOM Act—part of action that was taken, as I mentioned, just 2 months ago. Both Chambers of Congress and the President agreed it was time to end the bulk collection of American's call records pouring into the Federal Government.

I was a proud supporter of the USA FREEDOM Act and believed it was the right thing to do on behalf of U.S. citizens. My constituents all across Nevada—from Elko, to Reno, Ely, and Las Vegas—all understand how important these rights are and will not accept any attempts to diminish them. Today, I am here to continue protecting these privacy rights and uphold our civil liberties.

Protecting privacy will always be important to Nevadans. It is nonnegotiable to me, very important. Similar to many of my colleagues in the Senate, I believe addressing cyber security is also important.

When I was ranking member of the commerce committee's consumer protection subcommittee, I worked on these issues in detail. I understand very well the impact of data breaches, cyber threats. In fact, back in my State of Nevada, one of the top concerns is identity theft. Not only can these identity thieves wreak financial havoc on a consumer's life, but these threats also pose a serious national security concern.

We saw with OPM's breach that personal information for 21.5 million Federal employees, even those who received security clearances, was compromised. In my office, in fact, a member of my staff was breached three times in just the last 4 years. These thieves cross international borders. They break and enter into private homes. They hack their way to intrusion with a keyboard and a simple click of the mouse.

So I share the desire to find a path forward on information sharing between the Federal Government and the private sector as another tool in the cyber security toolbox, but I have always stood firm with these types of efforts that they must also maintain American's privacy rights.

The bill I see today, including the substitute amendment, does not do enough to ensure personally identifiable information is stripped out before sharing. That is why I filed a fix. Let's strengthen the standard for stripping out this information. Right now, this bill says the private sector and the Federal Government only have to strip out personal information if they know—if they know—it is not directly related to a cyber threat.

I would like to offer some context to that. Let's say you are pulled over for speeding, not knowing the speed limit does not absolve you of guilt. If your company fails to follow a Federal law or regulation, not knowing about the law does not exempt you from the consequences of violating it. Ignorance is no excuse under the law, so why should this particular piece of legislation be any different?

My amendments ensure that when personal information is being stripped out, it is because the entity reasonably believes—not knows but reasonably believes—it is not related to a cyber threat. One of my amendments addresses the Federal Government's responsibility to do this, and the other addresses the private sector's responsibility to do this.

This term ''reasonably believes''—let me repeat that—''reasonably believes'' is an important distinction that this bill needs. It creates a wider protection for personal information by ensuring these entities are making an effort to take out personal information that is not necessary for cyber security. Our friends over in the House of Representatives already agree the private sector should be held to this standard, which is why they included this language in the cyber security bill which they passed. I hope to see this important protection retained in any conference agreement should this bill move forward.

Furthermore, in a letter to a Senator last week, DHS directly acknowledged the importance of removing personally identifiable information and even went so far as to say this removal will allow the information-sharing regime to function much better. Even DHS agrees that with this amendment it would function much better. So what it comes down to is our Nation's commitment to balancing the needs for sharing cyber security information with the need to protect America's personal information.

I believe my amendment, No. 2548, to hold the Federal Government accountable strikes that balance, and I will continue strongly pushing forward to get this vote. I encourage my colleagues to support this commonsense effort to strengthen this bill and keep our commitment to upholding the rights of all U.S. citizens.

As we discuss this issue, I hope we will continue having the opportunity to truly debate and make improvements to this bill. I believe that if given the opportunity, we can strengthen this legislation even more to protect against cyber security threats while also protecting American citizens' private information.

No bill is perfect, as the Presiding Officer knows, but that is why we are here and that is why there is an amendment process. That is why I wish to see

the Senate openly debate and amend this bill, including my amendment. The privacy rights of Americans are too important an issue and a very important issue to all of us.

I acknowledge that some of my colleagues want the opportunity to debate issues related to the bill and those issues that are unrelated to the bill. I recognize there are many important issues Members would like to see addressed before August—or at least the August recess—such as my friend from Kentucky, who filed an amendment regarding firearms on bases. Like my colleague, I recognize the importance of this issue, which is why I introduced this legislation days ago. My legislation would simply require the Secretary of Defense to establish a process for base commanders in the United States to authorize a servicemember to carry a concealed personal firearm while on base. Men and women who serve our country deserve to feel safe and should be able to defend themselves while stationed in the United States. That is why I feel strongly that Congress should give our Nation's base commanders the authority they need to create a safer environment for our heroes serving across America.

At this time I recognize it is unclear if there will be an opportunity to debate this issue on this particular piece of legislation, but it is an important issue. Once again, I hope that as we continue to debate this bill that we will find a path forward on all amendments.

I appreciate the willingness of both Senator BURR and Senator FEINSTEIN to work with me on my amendments, and I look forward to continuing this debate.

I yield the floor.

The PRESIDING OFFICER. The Senator from New York.

Mr. SCHUMER. Mr. President, I ask unanimous consent that the next 30 minutes be equally divided between Senators SCHUMER, BOXER, WHITEHOUSE, MARKEY, and SCHATZ.

The PRESIDING OFFICER. Is there objection?

Mr. WHITEHOUSE. Mr. President, may I ask for a modification that I be able to speak for 1 minute on the cyber issue before we go into that 30 minutes?

With that modification, I have no objection.

The PRESIDING OFFICER. Is there objection to the request?

Without objection, it is so ordered.

Mr. WHITEHOUSE. Thank you.

Mr. President, in my 1 minute, I just wish to respond to what my friend, the Senator from Arizona, said. We are very keen to get a good, strong cyber security bill passed.

My concern about the amendment process is that amendments that will strengthen the bill and make it a better cyber bill ought to have a chance to get a vote. I have one that I worked out with Senator GRAHAM, who I think has good national security credentials and whom Senator MCCAIN respects, and another one with Senator BLUNT, who also has good national security credentials and whom I think Senator MCCAIN also respects. I believe both of the bills have now been cleared by the U.S. Chamber of Commerce, so they don't have a business community objection. But I also fear that if we followed the majority leader's proposal, he would file cloture and they wouldn't survive a germaneness test.

So I think our leader's offer, basically, of a specific list of amendments—none of which are ''gotcha'' amendments, all of which relate to this bill—would be a very good way to proceed, get on the bill, and get something passed.

The PRESIDING OFFICER. The Senator from New York.

Mr. SCHUMER. First, I thank my friend from Rhode Island. I think there is a broad agreement—I certainly do—that we want to move to this bill and, if given an agreement on a limited number of amendments, all relevant to cyber security, with no intention to be dilatory, and with time limits, we can get this done. But it is only fair on a major bill to offer some amendments and not just to fill the tree and have no amendments at all.

CLIMATE CHANGE

On the issue at hand, I thank Senators WHITEHOUSE, MARKEY, SCHATZ, and BOXER for speaking today and participating in this colloquy. I join my colleagues in appealing for meaningful action on climate change in this body, which thus far has been stymied by my friends on the other side of the aisle on behalf of special interests, and that is an absolute shame.

Climate change is one of the defining challenges of our time. Left unchecked, the changing climate and rising seas will threaten our shoreline cities and communities, as I personally witnessed after Superstorm Sandy buffeted New York. Left unchecked, a changing climate will have dramatic consequences for our children and grandchildren. Pope Francis's papal encyclical represents as much. He said climate change ''represents one of the principal challenges facing humanity in our day.''

We know we have to act. We know the American people want us to act. According to a New York Times-Stanford University poll, 74 percent of Americans said the Federal Government should be doing a substantial amount to combat climate change. That is 74 percent.

Democrats agree the Federal Government must do something. We tried to pass several bills through Congress, but my friends on the other side of the aisle blocked action time and time again on behalf of the special interests in the fossil fuel industry.

Now the President has a bold plan to reduce carbon emissions, which he announced yesterday and today, but already the groups on the other side are marshaling their forces. The New York Times reported today that fossil fuel lobbyists and corporate lawyers have been working since 2014, over 1½ years ago, to bring down these new rules.

Some of these Republicans admit that climate change is real and a threat. Yet they still block and block and block. My friend, the distinguished majority leader, has urged governors across the country to simply ignore the new climate rules while they cook up lawsuits to delay and frustrate their implementation.

OK. So you don't like the actions we propose or what the President proposes. Fine. What do you propose? I say to those on the other side of the aisle: What is your plan to meet this existential challenge? I have heard none. That is why this chart says:

—WANTED—

A GOP plan to combat climate change and reduce dangerous air pollution

#WhatstheGOPClimatePlan

There is none. We all know it is happening. Just look at the news, read the weather reports, and ask what scientists who are totally impartial and nonpolitical say. Unfortunately, I have a funny feeling that our colleagues on the other side are using the same playbook they are using on health care, immigration, and a host of other issues. Block, repeal, oppose, but propose nothing.

So I conclude my brief remarks by repeating the question. What is the Republican plan to act on climate change? Let me ask again in case they didn't hear me. What is the Republican plan to act on climate change?

Let me suggest that my friends on the other side join us in seeking solutions on climate change rather than obstructing our efforts and the wishes of the American people on behalf of special interests. Again, I thank my friends for organizing this colloquy.

I yield the floor.

The PRESIDING OFFICER. The Senator from California.

Mrs. BOXER. Mr. President, what is the order in terms of time allocated?

The PRESIDING OFFICER. Thirty minutes have been allocated. Each Senator has about 6 minutes to speak.

Mrs. BOXER. Will the Chair remind me when I have spoken for 5 minutes so I can wrap up?

The PRESIDING OFFICER. The Senator will be so notified.

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

In 2007, in its landmark decision called Massachusetts v. EPA, the U.S. Supreme Court found very clearly that carbon pollution is covered under the Clean Air Act. I think it is important to note that the Bush administration took the position that carbon pollution could not be covered under the Clean Air Act. They wasted about 8 long years litigating the matter, and we lost a lot of time. But when the Supreme Court finally spoke out, this is what they said, and I quote from the decision:

Because greenhouse gases fit within the Clean Air Act's capacious definition of ''air pollutant,'' we hold that EPA has the statutory authority to regulate the emission of such gases. . . .

Following the Supreme Court decision, the Obama administration issued an endangerment finding which showed that current and future concentrations of carbon pollution are harmful to our health. This finding built on the work of the Bush administration, and we found some of the raw data from the Bush administration, and we went public with it. This is what the endangerment finding said, among other things:

No. 1, severe heat waves are expected to intensify, which can increase heat-related death and sickness.

No. 2, climate change is expected to worsen regional smog pollution, which can cause decreased lung function, aggravated asthma, increased emergency-room visits, and premature deaths.

So once that endangerment finding was made, the Clean Air Act clearly requires the Environmental Protection Agency to act to control greenhouse gas pollution because it is determined that that pollution causes harm.

I wish to say, when I still had the gavel of the Environment and Public Works Committee, we called four former EPA administrators who served under Republican Presidents from Richard Nixon to George W. Bush. Every single one of those Republicans called on us to act now to reduce carbon pollution.

In that hearing, former EPA administrator Christine Todd Whitman, who served under George W. Bush, summed it up best—and I know my friends remember this. She said:

I have to begin by expressing my frustration with the discussion about whether or not the Environmental Protection Agency has the legal authority to regulate carbon emissions that is still taking place in some quarters. The issue has been settled.

This is a former Republican EPA administrator under George W. Bush. Continuing:

EPA does have the authority. The law says so, the Supreme Court has said so twice. That matter, I believe, should now be put to rest. Given that fact, the agency has decided, properly in my view, that it should act now to reduce carbon emissions to improve the quality of our air, to protect the health of our people and, as part of an international effort, to address global climate change.

Now, I was so proud in that particular hearing because I haven't found a Republican on the Environment and Public Works Committee who really even believes that climate change is real, to be honest. So to have a Republican—the former head of the EPA under George W. Bush—tell us it is time to move was very heartening to me because I believe action can't come too soon. The impacts that scientists predicted years ago are all around us and they are happening now.

I wish to share a couple of charts. The prediction quite a while ago was that we were going to see extreme heat more frequently all around the world. Well, 2014 was the hottest year on record, according to NASA and NOAA, and 2015, the first half of this year, is the hottest on record, according to NOAA.

Then, heat waves are more frequent. In Australia, in 2014, towns 320 miles northwest of Sydney hit 118 degrees.

The PRESIDING OFFICER. The Senator has consumed 5 minutes.

Mrs. BOXER. I thank the Chair.

Areas affected by drought will increase. Look at what is happening in my great State, the worst drought, according to scientists, in 1,200 years. Fires are increasing—same thing—and I am just so disheartened by the fact that we lost a firefighter, a visiting firefighter. Firefighters are fighting those fires right now and putting their lives on the line every single day. Tropical storms, hurricanes—this is all happening—heavy precipitation, flooding events. Houston got 11 inches of rain in 24 hours in 2015. And there is decreasing polar ice, and, in addition, rising sea levels.

So I will close with this. The evidence of climate change is here. To say you are not a scientist is no answer. We know you are not a scientist. Politicians as a group are not. But we should listen to the 98, 99 percent of scientists who are telling us our planet is in trouble. Our people are going to be in trouble.

As long as I can stand up on my feet in this body, I am going to stand shoulder to shoulder—well, not quite; in my high heels shoulder to shoulder—with my friends because this is a moment in our Nation's history when our kids and grandkids will look back and ask: Why didn't they protect us? Why didn't they save us? As far as I am concerned, it is our duty and our moral responsibility.

I thank the Chair, and I yield the floor.

The PRESIDING OFFICER. The Senator from Rhode Island.

Mr. WHITEHOUSE. Mr. President, I want to start my remarks with this photograph I have in the Chamber, which is a photograph of—I guess the miniplanet is what they call it now—Pluto. Why do I start remarks on climate change and carbon pollution with a picture of Pluto? I do so because of the amazing achievement it was for our NASA scientists to fly a craft close enough to Pluto to take that picture. That is a heck of an accomplishment by our American NASA scientists.

But that is not their only one. While this craft was shooting by Pluto taking these pictures, they had a rover rolling around on the surface of Mars. They sent a vehicle the size of an SUV to the surface of Mars and are driving it around. Do you think these scientists know what they are talking about when they say something as simple as climate change is real? Of course, they do.

But our Republican friends can't acknowledge that. They have even said these NASA scientists are in on a hoax. Can you imagine anything more demeaning to the people who put a rover on Mars and shot this picture of Pluto than to say: Oh, they do not know what they are talking about. They are in on a hoax. Forget about it. That is just not true.

The real issue is this. Here is Kentucky's electric generation fuel mix. That is its fuel mix. Guess what the gray is? Coal. That is basically all they have. There is a tiny little strip of blue at the bottom for the hydro. There is a little tiny strip here of red for oil. And there is a tiny little bit of natural gas here at the top, for which you need a magnifying glass. You can look and, with a magnifying glass, you can see this tiny little green line at the top that is their entire renewables portfolio. Really?

The last I heard the sun shines bright on my old Kentucky home. Right? So why no solar? None. How about wind? Do you think the wind blows through the Kentucky hills? None. You have to use a magnifying glass to see it. They are not even trying. They are not even trying. The coal industry has that State so locked down they are doing nothing.

Go to Iowa. There are two Republican Senators from Iowa—hardly some liberal bastion—and they get about 30 percent of their electricity from wind. It is not a Communist plot. It is not a Socialist fabrication. It is Iowa, and the farmers love it.

But no, we have to protect coal at all costs. So this is the GOP signal for what they are doing on climate change. I think it would probably be wise to take out the smile and actually put a little band of tape over the mouth so that it is clear that nobody is allowed to say a word.

This is really astonishing. Here we are, in which every State—just ask your home State university if climate change is real. You don't have to go far. Ask the University of Kentucky, ask the University of Louisville, ask your home State university. They know. Everybody knows. The problem is the coal industry and the Koch brothers have this place locked down, and it is ridiculous.

The Koch brothers have pledged to spend $889 million in this election through this group called Americans for Prosperity. And they have also said that ''anybody who crosses us on climate change will be at a severe disadvantage.'' When you are swinging a $900 million club and you are telling folks, disagree with us and you will be at a severe disadvantage, this is what you get—no plan on climate change.

You are going to hear endless complaining from our friends on the other side about the President's plan. What are you not going to hear? What their plan is. What is the alternative? What have they got? If you have nothing, if you have nada, zip, you really have to get into this conversation because even your own Republican young voters are demanding it. Republican voters under

the age of 35 think climate denial is ignorant, out of touch or crazy—their words in the poll, not mine.

So it is time we broke through. It is time the majority leader got away from this 100-percent coal situation that he is defending, allowed the future to take place, and allowed a conversation to take place here in the Senate. We are ready for it. We are ready for it.

I yield the floor to my wonderful colleague, Senator MARKEY, who has been working on this a good deal longer than I have.

The PRESIDING OFFICER. The Senator from Massachusetts.

Mr. MARKEY. Mr. President, I thank my good friend from Rhode Island, my friend from California, Senator BOXER, Senator SCHATZ from Hawaii, and all the Members who work on these issues.

This is the big one. This is the issue. This is the threat to the entire planet. Young people want us to do something about it. They are wondering when the older generation is finally going to get around to doing something about it, from moving to sending pollution up into the air to moving to clean energy, moving to new energy technologies.

So as they look at this, they look at coal, they look at a 19th century technology—coal—and they say: When are we moving to the new era? Well, that is a good question because in 2005 in the United States of America we deployed a grand total of 79 megawatts of solar. In 2014, we deployed 7,000 megawatts of solar—100 times more—because we started to have a plan.

Democrats put a plan in place by creating tax breaks for solar, by incentivizing more investment in solar across the country. Individual States started to put new regulations on the books—7,000 megawatts. Now we have 20,000 megawatts of solar in the United States. But we only deployed 79 in 2005.

Now, if you really want some great news as to what is possible, in 2015 and 2016, we are going to deploy 20,000 more—in just 2 years. So we are going to double the total amount of all solar ever deployed in the United States in just 2 years.

Over on the wind front, we are going to have about 80,000 megawatts total deployed by the end of next year, bringing it up to 120,000 megawatts. How much is that? When you look at a big nuclear powerplant and you see the picture of it, that is 1,000 megawatts. So we are talking about 120 of them being deployed by the end of next year.

So the young generation looks at us and they say: Can we do this? Can we meet the goals President Obama is setting? Can we meet the objective of having 28 percent of all of our electricity coming from renewables by the year 2030?

Well, if you hear from the coal industry or you hear from the nuclear industry, if you hear from the other fossil fuel industries, they say: Well, that is impossible. You can't do it. It is absolutely just going to be a very small part of the total amount of electricity that we generate in our country.

Well, they are just dead wrong. We are proving that in 2015 and 2016 because of the fight that is taking place at the State level—the tax breaks for wind and solar that were put on the books largely by Democrats here nationally. We are doing it. It is there. We now have over 200,000 people working in the solar industry in the United States. There are only 85,000 people who are in the coal industry. Got that? It is 2015. There are 80,000 people working in the wind industry in our country.

These are the growth industries. These are the Internet corollaries in clean energy. This is where young people are going. This is where innovation is going. This is where venture capital in America is going. This is where the innovation around our planet is going. We can do this. We can reduce greenhouse gases dramatically, increase employment simultaneously, and create wealth and health for our planet.

The President's plan will reduce by 90,000 per year the number of asthma attacks in our country. It will reduce by 90 percent the total amount of sulfur that is sent up into the atmosphere. It will be something that is supported by doctors and nurses and by Presidents and Popes. That is what we have. That is what this plan is. It is a beautiful plan. It is a plan that spans not just the technological and the political but also the moral imperative that is presented by this problem.

So yes, the big question that is being asked is this: Where is the Republican plan? Well, of course, there is none because they are still in denial that there is a problem, notwithstanding the fact that every single national academy of sciences of every single country in the world says there is a problem.

This is basically a small cabal of fossil fuel executives still trying to peddle 19th century technologies in the 21st century. It would be as though there were a cabal to stop us from moving from black rotary dial phones to wireless devices so that people could walk around with the new technologies. Oh, wait. There was a cabal. They fought it for years and years and years and years because they had the monopoly. The black rotary dial phone in the living room was all anyone would ever need. We had to break down those monopolies, and we have to break down these as well.

But here it is more than just having a phone in your pocket. Now it is actually saving the planet. It is ensuring we put in place the preventive measures that will reduce greenhouse gases while creating new jobs.

Senator WHITEHOUSE and I are part of a plan called the Regional Greenhouse Gas Initiative across New England, New York, Delaware, and Maryland. We already have a plan in place that has, in fact, reduced greenhouse gases, which has simultaneously seen dramatic increases in wealth, creating $1.5 billion in savings for consumers. We can do this. We can do this.

The auto industry said we could not increase the fuel economy standards of the vehicles that we drive. We just went right past them. The telecommunications industry did not want us to be moving to this wireless revolution. We just went right past them. The coal industry does not want us to act right now. For the sake of the planet, for the sake of generations to come, we must go right past them and ensure President Obama's plan is enacted.

I thank the Chair, and I now yield to the Senator from Hawaii, Mr. SCHATZ.

The PRESIDING OFFICER. The Senator from Hawaii.

Mr. SCHATZ. Mr. President, I thank the Senator from Massachusetts and Senators WHITEHOUSE and BOXER for their great leadership. I am really appreciative of the senior Senator from New York for taking the time to come to the floor to demonstrate his commitment to this issue.

There is an incredible opportunity here for American leadership. In Hawaii, in various places across the State, in 1 month we had 33 record highs—in the month of July. So we all know this is the challenge of our generation, and we all know the next most important step is the full implementation of the President's Clean Power Plan.

I wish to make a couple of points about the particulars of the plan. The first is that this is really done well. Normally, regulatory functions can be a blunt instrument. They can be a little less than careful in terms of how they are going to impact the economy. But this is done with great precision, with great care, and with great interaction with the incumbent utility companies and distribution and generation companies. So this is done with enough flexibility to say: Whatever your mix in terms of energies, we are not going to dictate exactly how you do it at a powerplant level, at a county level, at a city level. All we are saying is you have to meet these targets. And if you meet these targets through distributed generation or wind or solar or geothermal or hydro, that is not the Federal Government's concern.

Our concern is that carbon is a pollutant—and that has been determined by the courts, and it has been determined by scientists—and the Clean Air Act requires that airborne pollutants are regulated. So we are simply going to tell every State: This, like all other pollutants, has to be reduced over time.

I think the EPA took great pains to make sure this was done in a way that wouldn't cause too much upheaval in the economy. This is legally sound. There is no question that the EPA doesn't just have the authority and the discretion to move forward with carbon pollution regulations, they are actually required to under the last Supreme Court decision. And it is doable. Hawaii has a 100-percent clean energy goal. The Northeast has its RGGI program.

California has a cap-and-trade program. And all of our economies continue to grow. It is not that individuals and companies don't continue to have their challenges, but it is not because of our leaning forward into clean energy.

I will make one point about the kind of layering of obstruction. The first layer, which I think we have been successful in the last 6 months at breaking through, is the whole ''I am not sure whether climate change is real.'' Then they sort of pivoted to ''Well, I am not a scientist.'' So I don't think that is going to last for very long.

I think the next layer of obstruction is going to be ''I think climate change is real. I am not sure what percentage of climate change is caused by humans and how much of it is naturally occurring.'' I think we will be able to punch through that opposition.

The next layer of opposition will be this: ''America should wait.'' They will tell us that America should not lead in this, that we should wait for China, that we should wait for India, that we should wait for Germany, that we should wait for Japan. So let me ask this question: Since when does the United States wait for other countries to lead? This is the challenge of our generation, and it strikes me as preposterous that anybody who believes in American leadership would be willing to say ''Let's see what other countries do about this problem first. Why don't we give this a few years?'' We don't have a few years. This is an incredible opportunity for America to display the leadership it has always displayed in the international community. We finally have the high ground going into the Paris discussions. We are on legally sound ground, we are on morally sound ground, and I think politically we are increasingly on sound ground.

I am a full supporter of the President's Clean Power Plan. The one thing that causes me great dismay and I think causes some of the other participants in this colloquy dismay is that we are not even having a debate.

This is the Democrats asking you to come down to the floor and disagree with us. Disagree with the President. Disagree with Gina McCarthy. Tell SHELDON and me that our bill is a piece of garbage and this is what should be done instead. But let's have the great debate in the world's greatest deliberative body. Right now, it is entirely one-sided. If we are going to display American leadership, we need some Republican leadership as well.

Mrs. BOXER. Mr. President, will the Senator yield for a question? I don't know if the Senator is aware of this, but I do know Senators WHITEHOUSE and MARKEY know this since they serve with me on the Environment and Public Works Committee. Tomorrow morning at 10 o'clock, the Republicans on the Environment and Public Works Committee are going to put forward two bills, and they expect to pass them. One would stop the President's Clean Power Plan in its tracks without putting in anything to replace it—as a matter of fact, putting up obstacles, as I understand it, to any other plan. So it would stop it in its tracks and set up huge obstacles for another rule. The other one would say that if you spray pesticides on bodies of water and the pesticides get into the water, that spraying should be exempted from the Clean Water Act.

I mean, it pains me. It pains me to say that this is coming from the environment committee. Why don't they just rename it the ''anti-environment committee'' when they are in charge because every week, every day on the environment they go in the wrong direction for our children and our grandchildren. I know my friend has young children. I have young grandchildren.

Isn't it a shame that at the moment in time when the Environment and Public Works Committee—they did a great job—we did a great job, all of us, on transportation. We had a 20-to-0 vote. We are so proud of it. But on the environment, we are split down the middle, with Republicans trying to stop the Clean Power Plan, stop the advances in fighting climate change, stop the ability of regulators to protect the waters from pesticide spraying. Isn't it just shameful that this will be happening tomorrow?

Mr. SCHATZ. Through the Chair, I understand the time for the colloquy is about to expire. Just to respond to the Senator from California, if there is no objection, I would just say that we really do need Republican leadership here. Prior to about 10 years ago, the Republican Party had a long history and an august history of working with Democrats to protect our air and our water, and we are all sincerely hoping we can get back to that place.

I yield the floor.

The PRESIDING OFFICER. The Senator from New Hampshire.

PRESCRIPTION OPIOID AND HEROIN ABUSE

Ms. AYOTTE. Mr. President, I rise today to talk about a public health issue that is devastating communities and families in New Hampshire and throughout this country; that is, prescription opioid and heroin abuse.

I actually see my colleagues from Rhode Island and Massachusetts here. This is an issue where, on a bipartisan basis, we are focused on important legislation to address this terrible public health crisis.

Right now in New Hampshire, heroin—sometimes combined with a very powerful synthetic drug called fentanyl—is taking lives, ruining families, and harming communities. Public safety officials are confronting overdoses every single day.

My good friend, Manchester police chief Nick Willard, said recently: ''I'm up to my eyes in heroin addiction.'' Unfortunately, the statistics underscore Chief Willard's statement. In all of 2014, Manchester police seized over 1,300 grams of heroin. As of just last month, Manchester police had seized over 27,000 grams of heroin in 2015. That is nearly 26,000 more grams in just 7 months. In 2014, there were over 320 fatal drug-related overdoses in New Hampshire—up from 193 in 2013—and heroin and fentanyl were the primary drivers of nearly 250 of those deaths. In Manchester alone—our largest city—overdose deaths so far have increased 90 percent over 2014 and over 269 percent if we go back to 2013. That is the crisis we are facing. That is how many lives are being taken by opioids, by overdosing on prescription drugs and heroin, and it is devastating.

I worked with law enforcement when I was attorney general of New Hampshire. I know how hard they are working on this. They are working tirelessly to get these drugs off the streets. But they will tell you that we simply cannot arrest our way out of this problem. I have actually heard from law enforcement in New Hampshire that what they believe we need most to confront this public health crisis and to confront the public safety issues that go with it are more prevention, more treatment options, and more support for individuals in recovery.

We know that addiction to prescription pain medication can often become a gateway to heroin abuse. Unfortunately, right now the price of heroin on the streets has gotten so cheap that people are often going from prescription drug addiction to heroin addiction because of the price and the high and the way they feel. It is so tragic. According to a study from the Substance Abuse and Mental Health Services Administration, approximately 4 out of every 5 new heroin users previously used nonmedical prescription opioids before using heroin.

I wish to briefly mention two pieces of legislation that I believe represent critical steps in the right direction.

In February I helped reintroduce the bipartisan Comprehensive Addiction and Recovery Act. I thank my colleague from Rhode Island, who is in this Chamber, as well for his important work on this legislation. This legislation would expand opioid prevention and education efforts and expand the availability of naloxone to first responders and law enforcement. It would also support additional resources to identify and treat incarcerated individuals suffering from substance abuse disorder and encourage prevention by expanding drug take-back sites to promote the safe disposal of unwanted or unused prescription drugs, strengthening prescription drug monitoring programs, and launching a prescription opioid and heroin treatment and intervention program.

This summer I had the privilege of doing a ride-along with the Manchester fire department. Within half an hour of being at the fire department, we were called to a heroin overdose. I watched the first responders give Narcan to a young man who was on the ground who I thought was going to die, and he came right back. But what I noticed

was that in that room in a corner was an infant—an infant child whom the firefighter gave to another young woman in the room. Think about the impact of that. What chance does that child have when her father is on the floor, is not getting treatment, and is getting back in this cycle?

Often what I hear from our first responders is that when they save someone's life using a drug such as Narcan, they see the same people again because they are not getting the treatment they need to get the recovery they need from this horrible addiction they have.

Earlier this year I also reintroduced the Heroin and Prescription Opioid Abuse Prevention, Education, and Enforcement Act with Senator JOE DONNELLY of Indiana. This bipartisan bill would reauthorize programs related to prescription drug monitoring programs that are helpful to our physicians so they can get good information when they are prescribing pain medication; grants for local law enforcement; and establishing an interagency task force to develop best practices in prescribing pain medication.

The headlines we are seeing in New Hampshire every day in our local newspapers underscore the sad reality of this problem. Here are some we have seen in recent weeks:

The Union Leader: ''Mom, dad overdose on heroin while bathing child.''

The Nashua Telegraph in May: ''Nine die from drug overdoses in Nashua so far this year, including three in one weekend.'' Nashua is where I was born and where I lived.

The Telegraph on May 14: ''Toddler left in care of men, one of whom died of an overdose.''

There was more on that same day: ''Hampton man on heroin causes 5-car crash.''

May 29: ''Ossipee mom accused of selling heroin with 2 kids in the car.''

These news stories mirror the heartbreaking personal stories of loss I have been hearing about from families in our State. I want to share a couple of these stories.

Recently, I met with the family of Courtney Griffin, a 20-year-old young woman from Newton, NH. Tragically, Courtney lost her life to a heroin overdose last September. I was very moved by her family's story.

Courtney aspired to join the Marine Corps and had already attended boot camp. She was a charter member of the Kingston Lions Club. She played the French horn in high school and was a member of the tennis club.

During high school, Courtney started hanging out with a different crowd, and at some point the Griffins' prescription medication in their cabinet started disappearing. After Courtney graduated from high school, her addiction grew worse. She was stealing from her father's business and from her family in a desperate attempt to feed her addiction.

Courtney entered drug treatment, but she relapsed. When she finally admitted she had a problem, she tried to seek treatment but was denied coverage because the Griffins' insurance company said it wasn't a life-or-death situation. With some help from local law enforcement, Courtney was finally able to find a place to receive treatment. Tragically, she died of a heroin overdose about a week before she was set to begin treatment.

Her father Doug is doing everything he can to turn Courtney's story of tragedy into a cautionary tale so that he can save other families from what his family has been through.

Doug and others like him have a perspective on this crisis that is impossible for anyone who has not personally experienced a loss like this to understand. I admire his courage in sharing the story of his family so that he can save other families' lives.

Unfortunately, this story is all too common. In April, Molly Parks, a waitress at Portland Pie Company in Manchester, lost her life to a heroin overdose while she was at work. Her father is also speaking out to warn other families of the dangers of drug addiction.

I want to share as a final point one story that really moved me on Memorial Day. That story came from Keith Howard. He served our country with distinction. I know him personally. When he returned home from his enlistment, he struggled with alcohol and heroin abuse and he became homeless. Unfortunately, we hear too many of these stories about our veterans, what they are carrying with them, the wounds from war, and they become addicted to drugs and alcohol. Keith was one of those individuals who served our country and who became addicted. Today Keith is sober, and he helps run Liberty House in Manchester, NH, which provides sober housing for American veterans transitioning out of homelessness and helps our homeless veterans. Keith has dedicated his life to this.

On Memorial Day—on that important day on which we honor those who have sacrificed so much and made the ultimate sacrifice for our freedom—he shared stories with us of veterans who have come to Liberty House and turned their lives around, but he also shared stories of others who came but could not overcome their addiction, eventually costing them their homes, their families, and in some cases their lives.

Keith and Liberty House are doing incredibly important work for veterans in Manchester, but he believes there is more to be done. On Memorial Day of this year when we were honoring those servicemembers who gave their lives in service to our country, Keith reminded us of something else when he told a crowd at Veteran's Park in Manchester—and you could have heard a pin drop when he said this: ''Let us honor our dead by creating hope for our living.'' He is absolutely right.

It is clear to me that we need to work together. This is a bipartisan issue. This is a public health crisis. This is about the quality of life in our country. This is a problem on which we need to work together at the local, State, and Federal level in partnership to identify effective strategies to help save lives and take back our communities.

For my part, I will remain committed to fighting against this public health epidemic and taking it up at its roots to make sure for our children that this addiction and heroin—that we get it off our streets but that we get help for those who are addicted and that they understand they shouldn't feel the stigma I know many of them do, that we want them to come forward, we want to help them, and we understand this is incredibly difficult. We want them to know we stand with them so they can get the help and the treatment they need to lead productive lives.

Mr. President, I yield the floor.

The PRESIDING OFFICER. The Senator from Rhode Island.

Mr. WHITEHOUSE. Mr. President, before the Senator from New Hampshire leaves the floor, I wish to thank her for her work on the comprehensive Addiction and Recovery Act. She has been a very good partner in that effort. I know her home State, like Rhode Island, is suffering an extraordinary wave of opioid addiction and opioid fatalities. I know she is also working hard to make sure we get a hearing in the Judiciary Committee under present leadership. I am getting good signals on that. I hope we can pin that down before too long. I think this is a very important issue for us to get a hearing on, and I think it is one that all of the Presidential candidates are seeing. It is one so many of us see in our home States.

One of the smallest towns in Rhode Island is a little town called Burrillville. It is a beautiful place. It is in the northern rural area of our State. People laugh when I say ''the rural area of Rhode Island,'' but we really do have them. Burrillville is a very bucolic area, and there are very wonderful people there.

In the first quarter of this year, in little Burrillville, six people lost their lives to overdose. When I went to the Burrillville High School to do an event there about this bill and to listen and get ideas for our legislation, there were three recovering folks who came to talk about their situation. Like so many folks in recovery, they were unbelievably inspiring and noble in the way they discussed it. All three of them had gone to Burrillville High School.

It is a real problem, and I appreciate very much the leadership of the Senator from New Hampshire.

CLIMATE CHANGE

Mr. President, this is actually the time of the week for me to deliver my 109th ''Time to Wake Up'' speech. I find it a little bit frustrating these days because climate change used to be a bipartisan issue. Over and over again, we

had bipartisan, serious climate change bills. In fact, the first big climate change bill in the EPW Committee was Warner-Lieberman—John Warner, Republican of Virginia, and Joe Lieberman, Democrat of Connecticut. But then came Citizens United and all that dark money began to flow, all that fossil fuel money began to flow, all that Koch brothers money began to flow. Now, even as the evidence of climate change deepens to irrefutability, it is hard to find a Republican in Congress who will do anything. Here is the formula: Duck the question, deny the evidence, and disparage the scientists. Duck, deny, and disparage. That is some strategy for an issue which so many people take seriously.

As Congress sleepwalks through history, the warnings are painfully clear. Carbon pollution piles up in the atmosphere. Temperatures are rising. Weather worsens at the extremes. The oceans rise, warm, and acidify. These are all measurements. This isn't theory. The measurements confirm what the science has always told us about dumping so much excess carbon into oceans and atmosphere.

So hurray for the President's Clean Power Plan. For the first time, we have a national effort to reduce carbon pollution from powerplants, which are the largest source of U.S. carbon emissions. This plan is big. This plan is good. And this plan is urgently needed. I congratulate the President, I congratulate Administrator McCarthy, and I congratulate the good and public-spirited people of the EPA and other Federal agencies who worked hard to listen and make this plan final.

Of course, we will still have the usual complaining from all of the usual suspects. The Senate majority leader, the senior Senator from Kentucky, opposes any serious conversation about climate change. In fact, he is ready to lead his modern version of massive resistance against the Federal Clean Power Plan. The Republican leader has written to Governors urging defiance of the EPA regulations, calling them ''extremely burdensome and costly,'' which would be a more credible conclusion had he not reached it months before the regulations were even finalized.

Actually, if we want to get into the actual world here, a report just out from that famous liberal, Socialist bastion Georgia Tech found that the clean power rule could be enacted in a very cost-effective manner and could lower folks' energy bills in the long term. But let's not let the facts get in the way when there are fossil fuel interests to be placated.

As the Washington Post reported, folks expect to comply with the Clean Power Plan with relatively little effort, even in Kentucky. ''We can meet it'' is what Dr. Leonard Peters, Kentucky's energy and environment secretary, has to say about the Clean Power Plan. ''We can meet it.'' In fact, Dr. Peters praised the EPA for working with States like his to build this rule. ''The outreach they've done, I think, is incredible,'' he said. EPA had an ''open door policy. You could call them, talk to them, meet with them.'' The Kentucky experience was echoed around the country, as EPA listened closely to the concerns of utilities, regulators, experts, and citizens. They have made big adjustments to accommodate the concerns of stakeholders in the States.

When the usual complaining comes from the usual suspects, please ask them: What is your plan? How would you do a better job of addressing the carbon emissions that are polluting our atmosphere and oceans? What is your alternative?

Spoiler alert: You will look far and wide before finding a Republican plan. Don't look here. Don't look in the Senate. Republicans in the Senate have exactly zero legislation for addressing carbon pollution in any serious way. None. Zip. Nada. Duck, deny, and disparage is all they have. Don't look at their Presidential candidates. In recent weeks I have used these weekly climate speeches to look at Republican Presidential candidates' views on climate change. It is pathetic. There is nothing. What are we up to—87 Republican Presidential candidates? And not one has a climate change plan. OK, I was exaggerating about the 87.

Florida, ground zero for sea level rise, two Republican Presidential candidates, and what do the two of them have? Nothing. Republican mayors from Florida, State universities in Florida, the Army Corps office in Florida—nothing gets through to the candidates. Duck, deny, disparage is all they have.

The Wisconsin Presidential candidate ignores his own home State university, his own State newspapers, and his own State scientists. But Governor Walker can actually top duck, deny, and disparage. His response to climate change? Use your budget to fire the scientists at the State environmental protection agency.

How about our Presidential candidate, the junior Senator from Kentucky? What do we hear from him? He has said that the EPA rules are illegal, and he has predicted that they will result in power shortages—no lights and no heat. But does he have an alternative he would prefer? No. He has nothing, and, like all the other got-nothing Republican Presidential candidates, he is out of step with his own home State.

Kentucky isn't just easily able to comply with the Clean Power Plan; agencies and officials all across Kentucky are working seriously on climate change.

By the way, here is a look at why compliance is easy in Kentucky: Kentucky's fuel mix, which this charts, is a wall of coal. As the song says, the Sun shines bright on my old Kentucky home, but good luck finding any solar in there. You will need a magnifying glass to find this tiny little green line at the top that is barely visible that is solar and wind combined. I mean, really? Iowa can get to 30 percent wind. Iowa has two Republican Senators. It is not impossible. In Kentucky, they haven't even tried.

Kentucky's cities—Lexington, Louisville, Frankfurt, Bowling Green, and Villa Hills—get it. They have signed the U.S. Mayors Climate Protection Agreement in order to—quoting officials from Lexington—''act locally to reduce the impacts of climate change by lowering (manmade) greenhouse gas emissions.''

The hills of Kentucky are some distance from the shores of Rhode Island and the shores of New Hampshire as well. Living by the sea, I have to worry about climate change and what it is doing to our oceans and coasts. Kentucky is landlocked. So imagine my surprise to read the Kentucky Department of Fish and Wildlife Resources warning about sea level rise. I will quote them.

> With the predicted increases in severity of hurricanes and tropical storms, coupled with potential shoreline losses in Florida and throughout the eastern seaboard, people may begin migrations inland. If and when these events occur, Kentucky may experience human population growth unprecedented to the Commonwealth.

So I say to our candidate from Kentucky, the junior Senator, and our majority leader, the senior Senator, with Kentucky, their home State, projecting that people on the coasts will be hit so hard by climate change that we may have to flee inland to landlocked Kentucky, I hope the Senators from Kentucky will understand my persistence on this issue when their own State thinks that my citizens might have to flee to Kentucky to get away from this threat.

Kentucky is renowned for its horses. So I turned to Horse & Rider magazine and found a great article on ''how climate change might affect our horses' health.'' Horse & Rider's expert was none other than Dr. Craig Carter of the University of Kentucky. He had specific concerns in the article for equine health, but he also offered us this general reminder:

> It's not just horses (and people) at risk: crops are being affected, as are trees, due to beetle infestations. Climate change affects all forms of life.

That is from Dr. Carter of the University of Kentucky.

Kentucky Woodlands Magazine reports that ''the world is changing right before our eyes. . . . [O]ur natural systems are changing as a result of a warming climate.'' The magazine even warns that ''climate change is happening as you read this article.''

Meanwhile the Senators from Kentucky are not sure why that may be. The junior Senator has said that he is not sure anybody knows exactly why all of this climate change is happening. The majority leader invokes that climate denial classic: I am not a scientist. Well—and I say this thankfully—the scientists are here to help, including Kentucky scientists.

At Kentucky's universities, the science seems pretty clear about exactly why all of this climate change is happening. Dr. Paul Vincelli is a professor at the University of Kentucky Cooperative Extension Service. He says:

> In the scientific community, it is widely accepted that the global climate is changing and that human activities which produce greenhouse gases are a principal cause. Greenhouse gases have a strong capacity to trap heat in the lower atmosphere, even though they are present at trace concentrations.

Elsewhere, Professor Vincelli and his University of Kentucky colleagues write:

> Scientific evidence that our global climate is warming is abundant. . . . Practicing scientists consider the evidence of human-induced global warming to be extremely strong.

The University of Kentucky is not the only place. Eastern Kentucky University offers concentrations in environmental sustainability and stewardship, including courses on global climate change. Northern Kentucky University signed the American College and University Presidents' Climate Commitment, pledging Northern Kentucky University to ''an initiative in pursuit of climate neutrality.''

At the University of Louisville, Professor Keith Mountain is the chair of the department of geography and geosciences. He has lectured about ''how climate change is a measurable reality and how people have contributed to the trends.''

Despite all of the experts in Kentucky saying that human-caused climate change is real, despite the harms that State and local officials foresee for Kentucky and the rest of the country, and despite the easy steps being taken in Kentucky to comply with the President's Clean Power Plan, the Senators from Kentucky have no plan—nothing. They are part of the ''duck, deny, and disparage'' caucus.

And the Presidential candidates? There is almost nothing they won't make up to try to jam a sick in the wheels of progress—imaginary wars on coal when it is really coal's war on us, imaginary cost increases that have been completely debunked by actual experience, imaginary reliability failures when the real reliability problem is already happening around us thanks to climate-driven extreme weather. On and on they go. Yet they offer no alternative. Republicans simply have no plan other than a shrug.

Why do they have no climate plan? Why do they present nothing by way of limits to carbon pollution? Here is a clue: Look where the money comes from. It comes from fossil fuel billionaires and fossil fuel interests. Look at the beauty pageant hosted this weekend by the Koch brothers in Dana Point, CA, where Republican Presidential candidates went to display their wares to the big donors.

Do you think the Koch brothers want to hear about climate change? Here is another clue: Americans for Prosperity, part of the Koch brothers' big-money political organization, has openly warned that any client who crosses them on climate change will be ''at a severe disadvantage''—subtle as a brick from an outfit threatening to spend part of the $889 million total that the Koch brothers have budgeted for this election. And yes, $889 million in one election is big money. ''For that kind of money, you could buy yourself a president,'' said Mark McKinnon, a Republican and former George W. Bush strategist and a good Texan. ''Oh, right,'' he continued, ''that's the point.''

Even the Donald called the Republicans out on this one, calling the Koch brothers' California event a ''beg-a-thon,'' and saying: ''I wish good luck to all of the Republican candidates that traveled to California to beg for money, etc., from the Koch Brothers.''

What a shame, to be a Presidential candidate willing to ignore your home State universities, ignore your home State newspapers, ignore your home State scientists—unless, of course, you are trying to fire them—ignore your own home State farmers, foresters, and fishermen, all so you can prance successfully at pageants for the big-money fossil fuel interests that today control the Republican party. Duck, deny, and disparage is what gets you through the beauty pageant. So duck, deny, and disparage it is.

Eventually, the Republican Party is going to have to come up with a plan on climate change. The American people are demanding it, Independent voters, whom they will need in 2016, are demanding it. Even Republican voters demand it, at least if they are young ones. And it really matters that we get this right. It is the responsibility of the United States of America, as a great nation, to set an example for others to follow and not just sit back and wait for others to act.

Failing to act on climate change would both dim the torch we hold up to the world and give other nations an excuse for delay. Failure, I contend, when the stakes are so high becomes an argument for our enemies against our very model of government. How do we explain the influence of this special interest interfering with what must be done? There will be no excuse when a reckoning comes to say: I really needed the political support of those fossil fuel billionaires; so, sorry, world.

President Abraham Lincoln, a native Kentuckian, warned us that ''the dogmas of the quiet past are inadequate to the stormy present.'' Before the present gets too stormy, I urge my colleagues from Kentucky to heed the experts in their home State, heed the local leaders in their home State, and wake up to what needs to be done.

I yield the floor.

The PRESIDING OFFICER (Ms. AYOTTE). The majority whip.

Mr. CORNYN. Madam President, I came to the floor expecting to hear my friend and colleague talk about the bill that we are trying to get on, which is the cyber security bill, but again, I hear him returning to his favorite topic, which is climate change. I know he thinks that is the most important subject that we could possibly discuss on the floor of the Senate.

I will just say—and I certainly don't purport to be the expert he is—that when you look at the President's proposed new rules with regard to electricity generation, it looks to me like it is all pain and no gain. The experts, perhaps that he has referred to, said that CO_2 reductions would actually be less than one-half of 1 percent, and, of course, energy prices on low-income individuals, seniors, and people on fixed income would go up—people who have already been suffering through flat wages and slow wage growth for a long time. Of course, in this economy, which grew last year at the rate of 2.2 percent, it would be a further wet blanket on economic growth and job creation.

The Senator and I have worked together closely on a number of issues, and I enjoy his company, his intellect, and his energy, but I would say he is all wrong on this one. It sounds to me like so many of our colleagues sound like Chicken Little: The sky is falling, the sky is falling. Well, I don't think the facts justify it.

There are more important things we can do today and this week—for example, to pass a cyber security bill.

WORK IN THE SENATE

But first, I want to take a minute to consider what we have done this year under the new leadership. I know some like to focus on things that we haven't done, but I assure my colleague that we are just getting started, and there is a lot of important work that remains to be done. Last November the American people elected a new majority in the Senate, and I believe they elected us to represent their interests, to flesh out legislation, and to get this Senate back to work. We were elected to run the government and get things done; that is, of course, in a way that is consistent with our principles.

I even heard some people suggest that working with folks on the other side of the aisle in a bipartisan way is wrong, that we shouldn't do anything with Democrats on the Republican side or that Democrats shouldn't do anything with Republicans. That is a completely warped perspective.

I think the better perspective is that expressed by one of our conservative colleagues whom I asked when I got to the Senate: How is it that you work so productively in an important Senate committee with Senator Teddy Kennedy, the liberal lion of the Senate? This question was asked to one of the most conservative Members of the U.S. Senate. How can a conservative Senator and a liberal Senator work together productively to the best interests of their constituents and the American people? And he said: It is easy. It is the 80–20 rule. Let's find the

80 percent we can agree on, and the 20 percent we can't we will leave for another fight on another day. I believe we have been applying for the benefit of the American people the 80–20 rule, trying to find those things we can agree on, and we have been making substantial progress.

Since January we have delivered real results, proving that our back-to-work model was not just another empty campaign promise. Early this summer we passed the important trade bill, legislation that will help American goods get to global markets. Then we passed the Defense authorization bill, a bill that provides our men and women in uniform the resources and authority they need to keep us safe in an ever more dangerous world. We passed an important education bill, the Every Child Achieves Act, legislation that would actually do what my constituents in Texas want us to do, which is send more of the authority from Washington back into the hands of our parents, teachers, and local communities and out of the Department of Education here in Washington, DC. Just last week we passed the 3-year highway bill. Actually, it is a 6-year highway bill. We were able to come up with funding for the first 3 years and left open for us work to be done to come up with additional funding working with our colleagues in the House. Transportation infrastructure is something that supports our States and local communities and allows them to prepare for the growing infrastructure needs in the future while keeping commerce rolling, public safety protected, and protecting our environment.

Of course, we all know that we are just getting started. We have been here in the new Congress for 7 months. We are now on another important bill requiring every Senator's full and immediate attention. The Cyber Security Information Sharing Act is legislation that is long overdue. If it sounds familiar, it is for a good reason because we actually tried to pass this earlier this summer before it was blocked by our friends on the other side of the aisle. This legislation would provide for greater information sharing by people who have been subjected to hacks and would address the rampant and growing cyber threats facing our country.

One of the things that is so dangerous now is when a private company or an individual is hacked, they can't actually share that information through a central portal with other people to protect them if they haven't yet been hacked themselves. Of course, there are all sorts of concerns about liability and the like, but we need to address this to help the Nation deter future cyber attacks and to help the public and private sector act more nimbly and effectively when attacks are detected.

As I said, we had a chance to vote on this in June as an amendment to the Defense authorization bill. Unfortunately, this was about the time that some on the other side—I think most notably the next Democratic leader—announced something they called the filibuster summer. These are not exactly encouraging words when it comes to trying to work together to get things done. In spite of the real and frightening threats all around us, our Democratic friends filibustered that cyber security bill in June. We know what happened soon thereafter. The need for real cyber security legislation became even more apparent.

Many of us recall that in June there was an initial disclosure that hackers had accessed sensitive background information used for security clearance purposes at the Office of Personnel Management. The estimate in June was that about 4 million people were affected—their personal information. Then on July 9, after our Democratic friends filibustered the cyber security bill on the Defense authorization bill, there was a second report. This time that report informed us that more than 21 million people's private, secure information had been accessed. This information, illegally accessed, includes passport information, which would show anywhere and everywhere you have traveled; Social Security numbers, which are portals to all sorts of secure financial information; private information, background details, extensive information from previous places of residence. You can imagine. On a form you fill out in order to get a security clearance, you literally have to give your whole life history. That is the kind of sensitive information that was acquired on 21 million people as announced on July 9. Of course, it also provides the names of contact information, close friends, and family members.

While many of these reports indicate that China, one of the worst offenders along with Russia when it comes to malicious cyber attacks—many reports indicate China was responsible. The Obama administration for some reason has been unwilling to acknowledge that or tell us who attacked and accessed 21 million sensitive pieces of information. Of course, they have done nothing to respond to this growing threat of cyber attacks.

The Office of Personnel Management was not the only government agency affected. In early June, it was also reported that the Internal Revenue Service had similar problems and that data from more than 100,000 taxpayers had been stolen—again, the kind of information that if you were to disclose it about private taxpayers, it would be a felony. It would be a criminal offense. This is sensitive information that has now been stolen for 100,000 taxpayers. This breach included access to past tax returns, sensitive information such as Social Security numbers, addresses, birthdays—all stolen and potentially in the hands of criminals. It is exactly the kind of information that identity thieves want in order to pretend they are somebody they are not in order to steal your money.

Clearly, we don't have time to waste when it comes to cyber security legislation. I would point out that the Democratic leader himself, someone who is quick to dismiss the earlier vote when we tried to do this in the context of the Defense authorization bill in June, has said that he is committed to getting cyber legislation done. Well, I would ask: If not now, when?

This bipartisan legislation that passed the Intelligence Committee in the Senate by a margin of 14 to 1 provides us another opportunity this week. With cyber threats so clearly in evidence all around us, we should act quickly to implement a solution. I would encourage all of our colleagues to try to find that 80–20 solution on this bill.

No one is claiming it is perfect. I already talked to the committee chairmen in the House who say they have some different views, but that is customary around here. Once the Senate passes the bill, it can be reconciled with the differences in the House bill in a conference committee.

Surely we all agree that this type of legislation and the protection it provides is desperately needed. As the vote in July suggests, this is a bill in and of itself that will be the product of a functioning bipartisan Senate. Let's continue our progress for the American people.

I would add, by way of closing, that more than 70 pieces of legislation have passed the Senate since January 1, and 30 of those have been signed into law. More than 160 bills have been reported out of committee. That is what a functioning Senate looks like.

As I said before and I will say again, even our colleagues who are in the minority must enjoy getting to do what they were elected to do, which is to come here and cast a vote on behalf of their constituents on important issues that the Senate is addressing. I hope we can get this legislation passed this week.

Madam President, I yield the floor.

The PRESIDING OFFICER. The Senator from Michigan.

PLANNED PARENTHOOD

Mr. PETERS. Madam President, yesterday Republicans in the Senate put forward legislation to defund Planned Parenthood. Unfortunately, this bill was a clear partisan attack on access to health care for women, and especially women in rural and underserved areas.

One in five American women have relied on Planned Parenthood health centers at some point in their lifetime. Often, Planned Parenthood is the woman's only option for basic, preventive health care, including prenatal care, physicals, and cancer screenings.

For example, take Mary, a 20-year-old student in my home State of Michigan, who went through her campus health center when she found a lump on her breast. They told her it was nothing and not to worry. When she visited Planned Parenthood a year

later for an unrelated matter, the clinician expressed concern that the lump was still there. Through Planned Parenthood she got referred to a program for low-income women with breast cancer, and she received the treatment that she needed. Today, Mary is thankfully cancer free. Planned Parenthood provides upward of a half million breast cancer exams every year and can save the lives of women just like Mary across the Nation.

Planned Parenthood also provides about 400,000 potentially lifesaving cervical cancer screenings annually. Katie, another young woman from Michigan, went in for her annual exam at a Michigan Planned Parenthood center. Her exam revealed that she had cervical cancer, and Planned Parenthood helped her weigh options to cover the biopsy and subsequent surgery. Today she, too, is thankfully cancer free.

The doctors and nurses at these facilities provide affordable, potentially lifesaving health care to 2.7 million people per year. Michigan has 21 Planned Parenthood health centers, 11 of which are located in rural or medically underserved areas. These numbers mirror national numbers, with over half of their 700 health care centers located in areas with limited access to medical care. Federal funding for Planned Parenthood supports access to treatment at these health centers for women like Mary and Katie in States all across this country.

Let's be clear. Federal funding for Planned Parenthood or any other organization is not used for abortion. Let me say this again because it is a very important fact. Federal funding for Planned Parenthood or any other organization is not used for abortion. This has been settled Federal law for decades.

Despite this fact, we have seen the adoption of extreme measures that restrict a woman's fundamental right to make her own decisions about her reproductive health, including in Michigan. A woman should have access to reproductive health services and the freedom to make her own decisions about her health care, and I will fight to protect this right each and every day that I serve here in the U.S. Senate.

Yesterday evening I voted to stop the Senate from moving forward with legislation to defund Planned Parenthood. This bill would have jeopardized access to health care for 2.7 million men and women who rely on Planned Parenthood for their health care needs. While I am pleased that the Senate did not move forward with the bill, it is clear that we have not seen the end of these types of partisan attacks on Planned Parenthood.

I urge my colleagues to move away from efforts to restrict access to health care and, instead, focus on crafting bipartisan agreements to fund our government, provide certainty to American employers and workers, support small businesses, and grow our middle class.

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

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

(The remarks of Mr. HATCH pertaining to the introduction of S. 1922, S. 1923, and S. 1929 are printed in today's RECORD under ''Statements on Introduced Bills and Joint Resolutions.'')

Mr. HATCH. I suggest the absence of a quorum.

The PRESIDING OFFICER (Mr. PERDUE). The clerk will call the roll.

The legislative clerk proceeded to call the roll.

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

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

CLEAN POWER PLAN

Mr. MERKLEY. Mr. President, I rise today to join my colleagues in commending President Obama for putting forth his Clean Power Plan.

Theodore Roosevelt said:

> Of all the questions which can come before this nation, short of the actual preservation of its existence in a great war, there is none which compares in importance with the great central task of leaving this land even a better land for our descendents than it is for us.

I think it captured very well the challenge we face with carbon pollution and global warming because we are facing that great central task of leaving this land better for our descendents than it is for us.

We are facing a situation in which there is an accelerating quantity of carbon dioxide pollution in the atmosphere, and it is having a profound impact on, basically, the temperature of our planet. If we simply look at the carbon pollution itself, scientists have said that we are in trouble if it rises over 350 parts per million. Well, here we are with pollution that last year hit 400 parts per million. So we are above the danger zone. We are going deeper into the danger zone—let me put it that way—and that is not where we need to be.

Furthermore, we are accelerating the rate at which we are polluting the planet with carbon dioxide. It was just a few decades ago that the rate of carbon pollution was increasing by about 1 part per million per year, and now it is increasing by something closer to 2 parts per million per year. So where we need to be decreasing the overall pollution, bringing it down, we are increasing it and increasing the rate at which we are polluting, and that is a very bad place for humankind to be on this planet.

There is incontrovertible evidence of how quickly the planet is warming. We have, by scientific record—14 of the warmest 15 years in recorded history have occurred in the last 15 years. So 14 of the 15 warmest years over the centuries of measurement have all occurred in the last 15 years. That is not just one little warm spell on some little piece of land; that is a global temperature.

As carbon pollution is increasing, we see the global temperature increasing, and it is reverberating all across the planet. We see dramatic changes in the Arctic. The rate of warming in the Arctic is roughly four times the rate of warming in more moderate latitudes. So we are seeing an incredible decrease in the ice, huge changes that are coming so quickly, it is very hard for animals to adapt. Of course, people are well aware of the crisis the polar bears are facing, but that is just one particular visible species as an indicator of the challenges that are going on.

We are seeing the feedback mechanisms in the polar zone. We are seeing the open waters where ice is not reflecting the sunlight back up. More water is absorbing more sunlight, and that is creating an accelerated heating impact. We are seeing that as thawing occurs in the permafrost, we have these situations with what are called drunken forests, where the trees that all stood straight are now staggering in one direction or the other as they lean slightly, as the ground underneath them that was frozen is melting. As it starts to melt, it will start to release methane gas, which is a very potent global warming gas. So that is another feedback mechanism we should all be concerned about.

Let's take my home State of Oregon, and I think one could do this type of checkup, if you will, on any State in the Union. In my home State, we had a very severe series of droughts in the Klamath Basin, which is a major agricultural basin. We have had the three worst ever droughts in a period of 15 years. It corresponds with the period of the warmest years on planet Earth in recorded history. And that has a huge impact on our farming industry. So if you care about farmers, you should care about global warming.

Then we had a big challenge with our forests because as these summers are becoming dryer and as the types of storms we have are producing more lightning strikes, we are having a lot more forest fires. The fire season is getting longer and more devastating. Far more acres are being burned. Over several decades, the fire season has increased by several weeks in length, and the amount of acres burning each summer, on average, is increasing. So if

you care about timber, if you care about forests, then you should care about global warming.

Another impact of this changing pattern is that we are getting very little snowfall in the Cascades. Just as Glacier Park is now becoming the park of disappearing glaciers—you have to look very hard to find any glaciers left in Glacier Park—the Cascades also—a different mountain range—are losing their snowpack. In fact, we have virtually no snowpack now feeding the mountain streams that come down. So if you are a fisherman, you are looking at smaller and warmer streams, which is very unhealthy for fish.

That is not all. Right now we have sockeye coming up the Columbia River and getting to the Snake River, and they are dying because the temperature of the river is too warm for them to continue upriver to spawn. Some estimates that I have seen in the last week are that as many as 80 percent of the sockeye now returning are dying in the Columbia River before they make it to the Snake River. So if you care about fishing, you should care about global warming.

Then we look at our coastal shellfish and we discover that we have a significant problem with our oysters. Oregon produces a lot of oyster seed. Those are the baby oysters that get distributed to oyster fishermen. There is a similar process going on in Washington State at another hatchery. The challenge for the hatcheries is that the water that is pumped out of the ocean to produce the baby oysters, get them going, is becoming too acidic. This also is about global warming because the higher rates of carbon dioxide in the atmosphere are being absorbed by the ocean, and that creates carbonic acid. It has been enough that there is a 30-percent increase in the acidity of the ocean, and that is causing a big problem with baby oysters as far as forming shells. So if you care about the seafood industry, you should care about global warming.

When we talk about the issue of global warming, we are not talking about computer models and things that are 50 years into the future; we are talking about real-life effects seen on the ground right now, things that are having a big impact on our seafood, a big impact on our fishing, a big impact on our farming, and a big impact on our forestry. If you care about rural America's resource-driven economies across this country, you should care about global warming.

As a nation, it is incumbent on us to take on this challenge. We are the first generation—as has been said by others—to feel the impact of global warming and the last generation that can do something about it. It is incumbent on us, the Senators in this Chamber, the U.S. Senate, to take on this issue. It is incumbent on the Presidents and the executive teams they put together to take this on in partnership with the rest of the world because this is absolutely a tragedy of the commons.

Very clearly, if the United States takes some action to reduce our carbon dioxide or to reduce our methane production, it will have a modest impact but not enough. Nations across the planet have to act, and they will act more or less as a community because very few nations are going to say they will act alone knowing they won't have a big enough impact unless nations join together. So it is up to our leadership role in the world that we act actively, aggressively, and reach out with other nations to partner.

Earlier this year there was an agreement struck with China. China is going to produce as much renewable energy from electricity by 2030 as all the electricity we currently produce in the United States. I am not just talking about our renewable energy. If you take the U.S. renewable energy, our nuclear energy, our energy produced from gas-fired plants, our electricity produced from coal-fired plants, and you add it all together, that is the amount of electricity China is going to produce with just renewable energy between now and 2030. They are taking on a massive commitment to renewable energy. They wouldn't be doing it if the United States wasn't also responding aggressively. India is starting to become interested in doing their share, seeing that other nations are stepping up.

The United States should never be sitting on its hands and saying: We will wait for everybody else to act—not when there is an issue that threatens the success of the next generation of humans on this planet and the generation after and the generation after.

I said earlier that not only are we the first generation to feel the impact of global warming, but we are the last generation that can do something about it. What do I mean by that? What I mean is that the further you get into global warming, the further you get into carbon pollution, methane pollution, and more feedback mechanisms, the harder it is to stop. There is momentum that builds behind the warming of the planet. It becomes much harder to take it on. That is why we need to act decisively now.

So the Clean Power Plan the President launched, put forward yesterday, is responding to the moral demand of this generation to take on carbon pollution. It is doing so in a most cost-effective fashion, a fashion that will create jobs in the United States, a fashion that will reduce deaths in the United States.

Let me give an example of the health benefits. It will avoid up to 3,600 premature deaths, lead to 90,000 fewer asthma attacks in children, and prevent 300,000 missed workdays and schooldays. That is incredible. It will save the average family nearly $85 in their annual energy bill by the year 2030. So that is powerful.

In addition, we are going to create jobs in this fashion. It has the tremendous impact of putting people to work—tens of thousands to work, driving new investments in cleaner, more modern, and efficient renewable energy technologies.

I close by turning back to President Theodore Roosevelt, who said there is no more important mission than ''leaving this land even a better land for our descendants than it is for us.''

There are individuals who will come to this floor and they will say: Let's act someday but not now. Let's do it when it will not have an impact on jobs. Well, this will actually create jobs right now. Let's do it when it will cost less. Well, it never costs less if the problem gets bigger. It costs less to invest now. Let's pass it on to the next generation. They will solve it. That is morally irresponsible.

Every State is feeling the direct impact. Every rural community, timber community, fishing community, shellfish community, and farming community is feeling the impact today of our failure to address this yesterday. Our children, our children's children, and our children's children's children are counting on us in the Senate to act aggressively, to support a strong plan to take on carbon pollution—a strong Clean Power Plan. So let's do so.

I thank the Chair.

The PRESIDING OFFICER. The Senator from Oklahoma.

Mr. LANKFORD. Mr. President, I ask unanimous consent to speak as in morning business for 10 minutes.

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

ENERGY POLICY

Mr. LANKFORD. Mr. President, I come from an energy State—Oklahoma. We truly do all of the above. We have coal, oil, gas, wind, solar, hydro, geothermal, and we are just missing nuclear. Quite frankly, we probably would have nuclear if the regulations weren't so incredibly high and so incredibly expensive to do. In my State and in my region, we want diverse, inexpensive, healthy, plentiful, and reliable energy. We don't think that should be such a high goal that it is only limited to Oklahoma. Quite frankly, I think just about every area of the country wants that.

In fact, that used to be a bipartisan goal. It used to be that Democrats also supported ''all of the above'' energy. At some point, they shifted to the ways of Solyndra and determined if you want to be in that party, you have to commit to a certain environmental orthodoxy. It makes it a tougher conversation to have about real energy policy based around facts.

It is another day. It seems to be another day for the EPA to release massive new regulations. People wonder why their paycheck doesn't go as far nowadays, why food costs more, why products cost more, and why energy costs more. I can tell you why. It is this ever-growing regulation on the basic cost of energy. It changes the cost of everything.

The EPA stated they are not responsible for determining the benefits of

climate change, just that it would happen. As they put out their new Clean Power Plan, they said they didn't have to actually list or abide by the cost. They did determine the cost anyway—$8.4 billion a year to the American consumer; $8.4 billion on top of the energy regulations that already exist.

They also said they weren't responsible for having to be able to run through the actual effects on climate change, they just said it is happening and so we need to do something. In fact, it has been interesting for me to hear so many of my colleagues in the past 24 hours say: Republicans, put out your plan. We are doing something. You need to put out a plan to show you are doing something as well.

We ran the numbers on it and tried to evaluate it through the EPA models and looked for somewhere where someone who ran the EPA model would note how much change there would be in the environment if this plan is fully implemented. The model came back that it would slow the rise of the sea 0.3 millimeters once this is fully implemented—0.3 millimeters of sea change difference. To give an example, the head of this pen is 0.7 millimeters. So half the head of this pen is what we are going to save in sea level change if we fully implement this plan.

This seems to be about fear—severe weather, imminent danger. If you don't change everything in your life to the way we think you should live your life, the whole Earth is going to fall into chaos and ruin.

We need to have an energy debate on this floor. I completely agree. We even need to have a climate debate on this floor, but it doesn't need to be out of fear. It needs to be about the facts—what really needs to happen.

Let's start with some basic questions about energy policy and about energy future: What will it take to have reliable energy for the United States during a summer heat wave so we don't have rolling blackouts and senior adults suffering from heatstroke during an August afternoon?

What will it take to protect our grid so that doesn't occur? What will it take to have reliable energy for the hardest nights of winter to make sure Americans are protected in those coldest nights so their power doesn't go out because of rolling blackouts? What energy sources are plentiful in the United States and what energy sources leave us vulnerable to international pressures? What energy sources do we have that we should export to gain economic benefits and geopolitical power for the United States? What energy sources are economical so we can attract manufacturing to the United States to create more jobs for America? How can we ensure that the energy we use has the least amount of health risks so we can have a healthy nation and a healthy world? How about this question. What is the best way to keep energy diversity and distribution to protect our economy from rapid price swings or localized acts of terrorism?

That is how you begin to set an energy policy, which is to ask some general questions and then start answering some of those and asking, What is the best way to accomplish that? Instead, our energy policy is being run by environmental policy and fear of what could possibly happen in the future or protecting ourselves from 0.3 millimeters of sea rise.

Over the past 10 years, CO_2 emissions have drastically been reduced. Since 2005, CO_2 emissions from electric generation has been reduced by 364 million metric tons to 2,051 metric tons. The future goal, by the way, in this new Clean Power Plan is to have 788 metric tons of reduction from 2005, but we are already 364 metric tons there because there has already been a pretty dramatic reduction, much of that from a very slow economy—so 424 more metric tons by 2030. That would mean, even with an ever-increasing population, increasing energy needs, and hopefully a recovering economy, we need to cut much more.

Let me try to set this in context. I am going to throw around some numbers for a while, but I think we as a body can handle it. Let me give some perspective on where things are going on this.

The last time the United States emitted this target amount for CO_2 that has now been laid out as the targeted amount was in 1985, with 237 million people. If you want a little bit of throwback time, that is when Duran Duran, Huey Lewis, and the Commodores had all the big hits. That is when there were no personal computers or cell phones or iPads, cloud computing had never even been discussed, and there weren't all the electric devices we have now. We had 237 million people at the time.

The target is to get to that same amount of CO_2 usage, but we will have 363 million people at the time. That is the estimate from the Census Bureau. So the plan is to have 126 million more people emit less carbon and use less electricity. That sounds like an interesting plan. If you want the real number by percentage, let me break that down for you. In 1985, every 1 million people used 6.86 metric tons of CO_2—6.86 metric for every 1 million people. Now, in 2015, every 1 million people use 6.38 metric tons of CO_2.

That means, in the past 30 years, we have reduced for each 1 million people about half a ton of CO_2 because of energy efficiencies, because of the changes in the way we do energy. We do it much cleaner now than we did it in the 1970s and 1980s. Good for us. We achieved a lot in 1985—a lot of changes—but we have half a ton less CO_2 per 1 million people.

What the administration is proposing in their plan is that for every 1 million people in the United States in 2030, we would use 4.48 million tons of CO_2. That means, in the last 30 years, with the energy efficiency movement, with everything that has been done, with the remarkable shift in renewables, we have gained half a ton. The administration wants us now to get 2 tons of additional amount in the next 15 years.

Do you understand why a lot of people say this is just not rational? You can't get to an acceleration that fast with that big a goal. Here is what happens, though. I look at the facts and the requirements and immediately I am called a Neanderthal who just wants dirty air and dirty water. Actually, I have children, too, and I like clean air and clean water, but facts are very stubborn things.

A government mandate doesn't create reality. Remember Jimmy Carter in 1979? He declared his policies would create an energy path so that by the year 2000, 20 percent of America's energy would be produced by solar power—20 percent by the year 2000. How are we doing with that? Less than 2 percent of our energy in 2015 is produced by solar power.

Mandates don't create realities. If we drastically change all our electric generation to wind, solar, nuclear, and some natural gas, we will hit our annual number, but the amount of decrease per year will amount to approximately what China puts out in 1 month. You see, they are talking about reducing per year about 450-or-some metric tons of CO_2 that America would put out. China emits 800 metric tons per month. This is why so many people say this is a very expensive goal for America that will have no effect on the global reality.

Just to add a dose of cold water to the reality, it usually takes more than 10 years for a powerplant to even get a permit and start the construction because the Department of Energy, FERC, and EPA restrictions are so high. So this plan that in the next 15 years we are going to have all this rollout, we can't even get through the permitting time in that time period.

I haven't even touched on the legal issues of the new mandates of the administration. They haven't been in front of the American people or in front of the Congress. The existing law—the Clean Air Act—does not allow EPA to add another layer of regulations on top of the existing regulations. That is clear in the law. You cannot do that. Even the former Sierra Club general counsel, David Bookbinder, found this new proposal is based on what he called a ''legally dubious ground.''

As a nation, we don't need more pie-in-the-sky energy ideas. We need real solutions and a right direction that will benefit the United States and the world. We lead the world in power and ideas. We should set high goals. But our goals should help us as a nation, not hurt us. Every American pays more at the pump right now because of the increasing regulations in the ethanol mandates. Every American is paying more for gasoline than we should. Every American is paying more for electricity than we should because of

the cost of all these mandates. People ask me all the time why their dollars don't go as far; the regulations are the reason.

Many people want to talk about our energy future—great, so do I. But I also want to talk about our energy present. The goal of a quarter of America's electricity produced by renewables is a good goal. It is a huge jump. We are just at around 5 percent right now in renewables. But that will still leave us—even if that goal is accomplished—with 75 percent of our energy coming from coal, oil, natural gas, and nuclear. That is base power. It is not effective at night or on hot still days in the summer when the wind doesn't blow. It is base power.

Solar is more efficient than ever. Let's keep going. It is a good thing. I am glad we are able to harness some of that. It takes a massive amount of acreage. There is a new solar facility that just came into Oklahoma. Great, we are glad to have it. It has 15 acres of solar—15 acres of panels. It powers two neighborhoods—two neighborhoods—and it takes 15 acres to get that accomplished.

Windmills are much more efficient right now than they have ever been. In fact, they are efficient enough that we should probably stop subsidizing them. They are not a startup anymore. We started subsidizing utility-grade windmills more than 20 years ago, saying someday this thing is going to be efficient enough that it is going to work. I think we are already there. In fact, there are more than 48,000 utility-scale wind turbines in the country right now—48,000 windmills in the country right now. To give some perspective, there are 36,000 McDonald's in the world. We have 48,000 windmills. There are 36,000 McDonald's in the world. I don't exactly think the windmill thing is a startup anymore. I think maybe that is fairly well established. So maybe the need for the subsidy is not there.

Geothermal is a great energy source. We have yet to tap the full potential for heating and cooling our homes and businesses. But we still need natural gas, oil, coal, and nuclear to provide power for the foreseeable future. Even the Obama administration lays out over the next 30 years what they anticipate energy use will be, and they still anticipate we are going to need gas, coal, oil, basic base power.

So let's do it the cleanest way we can, the most efficient way we can so the consumer is not punished for using energy. We should keep innovating for the future, but we should make rational choices on energy.

Let me give an example of an irrational choice. Can I do that? Here is an example of an irrational energy choice: the Keystone XL Pipeline. Now, I know everyone is going to say we are going to talk about Keystone again. This is day 2,510 of a permit request to build a pipeline. Today is day 2,510 of a permit request sitting on the President's desk for a pipeline. Let me give an example.

All of these black lines that we see here are crude oil pipelines in the United States currently there. This is how many thousands of miles? More than 60,000 miles in the United States of crude oil pipeline—60,000. It is another pipeline. Why does it take 2,510 days to be able to make a decision on this? Oh, it is an international pipeline. That is right. Well, let me add something to it. We have 19 international pipelines currently running—19 of them. This would be No. 20. This is not something new and radical. We are already buying a significant amount of Canadian oil. That oil is coming from right up here. Look at all of these pipelines already coming from the same spot. Look at that, they cross the border, and it has been safe and reliable. This has not been a big challenge for us.

That oil is not just being blocked from Canada. Many people think that if we don't put in a pipeline, it won't come. Actually, it is coming by rail already. It is already moving into the country. This is just cleaner and more efficient to be able to move it that way. Canada is discussing taking a pipeline and bringing it all the way over here, dropping it off and bringing it to the coast, and bringing it by ship over to the U.S. gulf coast.

Does someone think that is more efficient than bringing a pipeline in? Now, it is not more efficient by rail. It is not more efficient by this way. If we are going to bring it in and Canada is going to sell it, why don't we have an international pipeline—that No. 20, right there—and be able to bring it in?

Now, I have heard multiple people say it is because of the aquifer in Nebraska. Let me try to discuss this because I have heard this over and over: We can't run pipelines because of the aquifer in Nebraska.

Here is the aquifer that is being discussed all in the purple here. Every line that we see is an existing pipeline running through that aquifer. This tiny blue line is the proposed Keystone that is to go right through there as well.

They make these comments: We can't run it through the aquifer because, oh, my gosh, we can't run a pipeline there. That is how many we already have in that spot. This is not radical. This is not different.

In fact, let me give one more image. This is the number of pipelines that we have in America right now of all types. This is both natural gas and crude and all kinds of petroleum products that move through the United States all the time—every single one of those lines. This is irrational energy policy that is knee-jerk that is happening. To say that we can't add one more pipeline because somehow that would go over the top ignores the reality of what we already have in the United States.

Moving energy by pipeline is clean and efficient. It is also a rational way to do it. We have to move from fear-based energy policy to fact-based energy policy—to look not only at our energy future but what may happen in the decades to come. I hope my car one day runs on a pinwheel on the hood ornament. That would be great. But that doesn't happen right now. My car still runs on gas. So does everyone else's here. And for every single person here that gets on an airplane every week, it doesn't run on water. It still runs on energy that we pull out of the ground.

So for the foreseeable future we need to deal with the facts. Stop hurting consumers for some proposed future hope of what may happen. Let's do it clean. Let's do it innovative. But let's not hurt consumers in the process.

People want to know where their money has gone. It is being spent away on regulations. Let's get to work on an energy plan.

I am glad to have this conversation, but this should not be a conversation in the hallways of the EPA. This should be a conversation in this room to determine where energy policies go.

I yield the floor.

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

Mr. PERDUE. Mr. President, I ask unanimous consent to speak for up to 10 minutes as in morning business.

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

ECONOMIC GROWTH

Mr. PERDUE. Mr. President, I rise today to speak about seizing the opportunity to drive real economic growth right now. But first, I wish to give a little context by referencing our great Nation's desperate fiscal condition.

Decades of overspending by both parties and mismanagement by both parties have led to a crushing $18 trillion of Federal debt. Even more sobering to me is the upcoming over $100 trillion of future unfunded liabilities coming at us like a freight train. We have a fiscal crisis in this country. Everybody can see it. People back home can feel it. As an outsider, my role is to bring a new sense of urgency to Washington to help solve this fiscal crisis.

While I am encouraged by the work my colleagues on the Budget Committee completed this year—we completed a balanced budget for the first time since 2001—it was merely a good first step in the right direction. But we have a lot of heavy lifting to do. We must act right now to get our fiscal house in order before it is too late.

Yes, we must cut unnecessary spending. Yes, there are redundant agencies and programs that should be eliminated. And yes, we do need to have a national dialogue on how we keep the commitments that were made to our seniors, while saving those important programs for future generations. However, discretionary spending cuts and long-term reforms to mandatory programs alone will not solve this problem. The numbers just simply don't add up to solve this crisis. Economic growth is really the only answer.

Economic growth supports good-paying jobs across the entire country, and economic growth eventually means

more revenue for the Federal Government without raising taxes. If we are ever going to get out of the hole that Washington has dug for our country, we are going to have to grow our way out of it economically. One of the biggest opportunities to infuse energy and investment into our economy right now is before us as I speak, just waiting for us to act on it.

There are approximately $2.1 trillion in corporate profits of American multinational companies sitting abroad trapped by our archaic tax laws. Imagine if we could lure just a portion of that back in terms of capital investment in our economy. The multiplier effect alone would be incredible as it rippled its way throughout our domestic economy.

In recent weeks we have heard a lot of talk about how we in Washington can get those overseas earnings repatriated back into the United States economy. For me, the solution is quite simple. We simply eliminate the barrier to repatriation by completely eliminating the tax on repatriation.

My approach isn't just based on my business career. It is not just based on my desire to give our economy a much-needed shot in the arm. Completely eliminating this tax on repatriation is an absolute necessity for global competitiveness and to create a level playing field with the rest of the world.

I rarely compare other countries to the United States for simple reasons. No. 1, we have an 18 trillion economy. No. 2, we are the innovator in the world. No. 3, we have the rule of law. No. 4, we have really a very dynamic and diverse economy. Very few countries compare. But this is one time where a comparison is warranted because it is about how we compete for economic development and jobs with the rest of the world.

A company headquartered in the United States not only has to pay taxes in every single country in which it does business, but when it elects to bring back the remaining profits from abroad, that corporation is forced to pay an additional tax—a repatriation tax. This doesn't happen if the corporation is based in Canada, France, Germany, the United Kingdom, Australia, Japan or, indeed, the remainder of the 39 OECD countries. In fact, there is only one country on the list of 39 OECD countries that has a repatriation tax—the United States. The United Kingdom actually eliminated their repatriation tax in 2009, and over the last decade they have reduced their corporate tax rate from 28 percent to 18 percent.

We continue to see companies leave the United States because they can go pretty much anywhere else and benefit from much lower tax rates than here in America. We have seen a rash of those inversions over the last few years, and it is not going to stop until we deal with the underlying problem; that is, our corporate tax rate is not competitive with the rest of the world. The repatriation tax is a derivative of that primary causal problem.

What I am talking about today is simply the elimination of the repatriation tax. But sooner or later, we have to deal with the fact that our corporate tax rate is simply not competitive. The question simply before us is, Do we want multinational companies—in many cases iconic American brands—to continue to call the United States home or not?

As a former CEO of a large branded company that manufactured in dozens of countries and sold in dozens more, I have firsthand experience, and I can tell you that, based on that experience, we are losing our competitive advantage with the rest of the world. In fact, I see us now at a growing disadvantage for our American companies to compete with companies in other countries.

The hostile regulatory environment the current administration has created is killing American jobs, and our outdated tax system is forcing them to expand abroad. Executive orders and regulatory mandates have created a punitive atmosphere in which to try to grow businesses or start businesses here in the United States. Unfortunately, in typical Washington fashion, the dialogue on repatriation is focused on how to get a short-term solution—a short-term Federal tax increase—instead of using repatriation as a tool to grow the economy and make us more competitive. In my estimation, this kind of thinking is dead wrong and another example of how we got in this mess in the first price.

We should not be looking at repatriation as a way to pay for the highway trust fund or any other short-term solution to Washington's spending problems, for that matter. That kind of shortsighted thinking will only make our fiscal situation worse. It will only cause more American companies to look for a new home.

Repatriation is a big idea with a big potential impact for our economy. If we encourage repatriation the right way, it means sustained growth for our economy. It means more American jobs and innovation. Ultimately, it means an organic increase in Federal tax revenue based on pure economic growth. This growth can allow us to deal with our economic and fiscal priorities and finally develop a long-term plan to begin to pay down our overburdened debt.

Before I conclude, I have one final thought. I hope this thought will compel my colleagues to act with a sense of urgency on this issue and others that impact our economy. We actually have fewer people working than at any time in the last 30 years. When I go back home, the number one question that is put before me is: How can I get my hours up? How can I get more work?

People back home know we have a crisis. It is not just bureaucrats in Washington looking for a few more tax dollars so we can make government bigger. This is about putting people back to work—helping us compete against the growing economies of China, India, Russia, and other rivals in today's world.

The approval rating of Congress today is somewhere in the mid-single digits, and that is only because our mothers voted. I believe it is because this town's priorities are not aligned with those of the people who sent us here for their bidding. Folks back home know that shortsighted, short-term solutions to the big problems are how Washington got in this mess in the first place.

Today we can continue to argue about temporary ways to pay for trust funds that are going bankrupt every few weeks, or we can simply finally get serious about solving this systemic problem before we have to hand it to our children and our children's children. I know the American people expect the latter. In fact, they are demanding it. That can happen, but we must make real tax reforms right now that will set us on a new course for economic growth and opportunity for generations to come. The time for serious debate about repatriation has come.

We have an opportunity. I implore my colleagues in the Senate to debate this earnestly, and let's move on this right now and put people back to work and make America more competitive for our children and our children's children.

I yield the floor.

The PRESIDING OFFICER. The Senator from West Virginia.

ARENA ACT

Mrs. CAPITO. Mr. President, yesterday President Obama and his Environmental Protection Agency announced their final clean power grab, continuing the economic assault on energy-producing States like West Virginia.

Yesterday, Alpha Natural Resources, one of the Nation's largest coal producers, filed for bankruptcy. As of the end of 2014, Alpha had 4,870 employees at 33 active mines and 13 prep plants in West Virginia. Alpha follows Patriot Coal, Jim Walter Resources, and James River mining—all of which have filed bankruptcy since 2014.

According to the Mine Safety and Health Administration, coal mining employment has dropped from 143,437 in 2011 to 98,310 in the first quarter of this year. That represents a 31-percent drop over the last 4 years.

Earlier this year when Murray Energy announced hundreds of layoffs in northern West Virginia, the Wheeling Intelligencer newspaper reported that the impact would mean almost $62 million in annual income lost wages for Ohio Valley residents. Other communities have also been hard hit. Nicholas County—a small county in my State—was forced to lay off sheriff's deputies because they could no longer pay their county commitments because of a decline in coal severance revenues.

Now, 17 coal units in West Virginia have retired due, at least in part, to

EPA policies. The electricity produced by these units is enough to power 2.7 million homes. Put another way, the units that have already closed in West Virginia would generate enough electricity to power the entire State of Hawaii.

These are not the same old talking points, as the administrator of the EPA and the President said. These are not stale. This is not motivated by special interests. These are real Americans, real jobs, real families, and real communities that have been negatively impacted by this administration's overreaching regulations. These are people like Tammy Rowan of Coalton, WV, who wrote me a letter:

> My whole family has concerns with the regulations that seem to be out of control. EPA, government officials, and the president are putting families out of work.

Or Patrick Sparks in Warriormine, WV, who said:

> I know the EPA has been trying to force strict regulations on coal. It's hurting a lot of people, not just here in West Virginia, but a lot of businesses are suffering from it.

And Theresa Simmons of Tridelphia, WV, whose family has worked in coal mines for generations, wrote:

> My husband was able to provide for our family with just his income. We were able to donate money to local charities and help needy families around the holidays. Now that is going to be my family, looking for donations.

Put simply, yesterday's announcement will make an already bleak situation in our State much worse. Working families across the Nation woke up to the sad news that their jobs just don't count. Much has been said about the open process that led to this final rule. In fact, West Virginia, which is one of the States most deeply affected by this regulation, was not even visited by the EPA after I and others extended many invitations. Instead, they went to cities like Chicago, Boston, and San Francisco. Talk about special interests. Talk about being bold.

The administration's final clean power grab will force States away from affordable, reliable energy toward expensive, intermittent power sources, many of which are heavily subsidized by the taxpayer. It proposes benchmarks that are more stringent and less attainable.

In West Virginia, our emissions rate under the proposed rule was to drop 20 percent. On Monday, the final rule requires our rate to drop by 37 percent—a drop that is almost twice as severe. There is no way for West Virginia to comply with this rule without significant cuts to our coal production, coal jobs, and coal use.

According to the EPA's own calculations, the final rule is worse for coal than the proposed rule. Coal's share of electric generation will go to 27 percent by 2030 under this rule—as compared to 39 percent, which we currently have or did have in 2014.

If this misguided final rule is ever implemented, pain will be felt by all Americans with fewer job opportunities, higher power bills, and less reliable electricity. Studies of the proposed rule projected that the Clean Power Plan will increase electricity prices in a State like mine 12 to 16 percent.

What does this mean for American jobs? A recent study by the National Rural Electric Cooperative Association found that a 10 percent increase in electricity prices can mean as much as 1.2 million jobs lost. Roughly one-half million of these job losses will be in rural communities like those in West Virginia. Put simply, affordable energy matters. It especially matters to those who the administration incorrectly says will benefit the most from this rule, which is the low and moderate income.

More than half of West Virginia's households take home an average of less than $1,900 per month and already spend 17 percent of their income on energy. These families are especially vulnerable to the administration's clean power grab. While States are given additional time to comply under the final rule, it does not change the fact that the EPA is picking winners and losers in the energy economy. The losers will be the American families who rely on affordable and reliable energy. We can and we should innovate for the future but not with a sledgehammer bearing down on us. Thankfully there are several legislative options that Congress can pursue to challenge this rule.

Tomorrow the EPW Committee will be taking up my legislation—the ARENA Act. Let me explain that briefly. This bipartisan legislation would empower States to protect families and businesses from electric rate increases, reduced electric reliability, and other harmful effects. It will force the EPA to reconsider this misguided rulemaking.

The ARENA Act holds the EPA accountable by requiring the agency to issue State-specific model plans demonstrating how each State will meet the required reductions. It gives States the ability to opt out if the plan hinders economic growth.

For existing powerplants, the ARENA Act delays implementation of the Clean Power Plan until the courts determine the legality of the rule. Recently, the Supreme Court ruled that EPA had unlawfully failed to consider costs when formulating its MATS regulation. Because the rule went forward while it was still being litigated, millions of dollars were spent to comply with a rule that was ultimately deemed illegal. States should not be forced to proceed until the legality of the rule has been determined. I hope that many States will follow Leader MCCONNELL's suggestion and delay implementation of this rule until the legal process is completed.

Mr. President of the United States, your clean power grab will devastate already hurting communities in my State. It will cause economic pain for working families across the country. It will forever harm our energy landscape.

The proposed rule was bad. The final rule announced yesterday is even worse, doubling down on the destruction of our economy. There is no question that we must take steps to protect our environment, but it simply cannot be at the expense of our families.

We can do better. Let Congress, the elected representatives, make these decisions. That is the way it should be. I ask my colleagues to join me by supporting the ARENA Act and sending these overreaching EPA regulations back to the drawing board.

The PRESIDING OFFICER. The Senator from Oregon.

WILDFIRES IN THE WEST

Mr. WYDEN. Mr. President, as the Senate prepares for the month of August in our home States, I want to discuss tonight what I believe to be an urgent issue: The West is on fire. There is a really serious prospect that my part of the country is going to get hit by what I call the terrible trifecta—drought, high temperatures, and enormous fuel load on the forest floor. When you couple that with a lightning strike—which is not exactly a rarity in my part of the world—all of a sudden you can have on your hands an inferno. The fires are getting bigger, they are lasting longer, and they are doing more damage.

Senators here on both sides of the aisle—Democrats and Republicans—have come to realize that our system for fighting fire is a broken, dysfunctional mess. What happens is, historically, prevention gets short shrift. The agencies can't do enough thinning; they can't do enough of the preventive work to reduce the fuel load on the forest floor. Then you have one of those lightning strikes, and all of a sudden there is a huge fire because the fuel buildup is so great on the forest floor.

The agencies then run out of money putting these fires out because they are getting bigger, and they are lasting longer. The problem just keeps getting worse because the agencies then have to rob the prevention fund in order to fight these big fires. In other words, the agencies borrow from the prevention fund, and the problem gets worse because by shorting the prevention fund it creates the prospect of still more big fires in the future.

With the West burning, the Western Governor's Association—a bipartisan group—put out a new update of how big the recent fires are. So far in 2015, nearly 6 million acres have burned. That is an area bigger than the State of New Jersey, scorched in massive fires.

In my home State, a wildfire in Douglas County in southern Oregon has spread to over 16,000 acres, with 1,400 crew members battling a blaze that is threatening more than 300 homes. According to recent reports, 20,000 acres were scorched by one single fire in northern California in a matter of only

5 hours. That is 20,000 acres—nearly the size of the entire city of Bend, OR—that burned in the time span of an extra-inning baseball game.

With the Forest Service budget effectively flatlined and the higher cost of fighting fires producing this robbing of other programs that I have described—the fire borrowing—what you have is a vicious, self-defeating circle of firefighting and shoddy budgeting, which, in effect, will cause an even bigger crisis in the future because you shorted the prevention fund. In 10 years, if this isn't fixed—what is known as fire borrowing—the Forest Service says it will be spending two-thirds of its entire budget on suppressing wildfires, and my constituents say they will be calling the Forest Service the Fire Service because that is essentially what they will be.

This is particularly serious right now, which is why I came to the floor tonight to try to drive home the urgency of this issue, because it is so dry in the West. This year Governor Brown of my home State has declared drought emergencies in 23 of our 36 counties. All 36 counties are experiencing severe drought, according to the National Drought Center. It is a very dangerous mix of factors, what I have come to call the terrible trifecta of drought and temperatures and fuel load. They all came together and turned the West into a virtual tinderbox.

To try to fix this, my colleague Senator CRAPO and I have worked together for quite some time to in effect say that what we ought to do is break this dysfunctional system of fighting fires and go with a different approach. What we would say is that the biggest fires—the 1 or 2 percent of the megafires—we ought to fight them from the disaster fund because they really are disasters. Use the prevention fund for what it is intended, which is prevention, so we can keep from having those megafires.

The good news is that the Congressional Budget Office—my colleague is new here, but he already knows that the Congressional Budget Office is our official scorekeeper—says that there really aren't added costs for this approach because while you would spend a bit more money trying to put out those megafires, you would save some money by not cheating the prevention fund and not having so many fires in the first place.

In effect, it is a lot smarter for the agencies to focus on keeping our forests healthy and clear of the fuels that go up in flames when lightning strikes. So we do the preventive work and we no longer are shorting it by all the fire borrowing which I have just described.

Senator CRAPO and I have been able to get well over 250 organizations to go on record in support of our idea. These are groups associated with forestry policy, environmental folks, industry personnel, people across the political spectrum. More than 250 groups have said they are in support of this. The Under Secretary of Agriculture, Robert Bonnie, noted in a recent letter that the proposal Senator CRAPO and I have offered is one that both fixes fire borrowing and provides the resources needed to prevent these catastrophic wildfires down the line. Fifteen of our colleagues here in the Senate have supported the bill, and 123 Members in the other body have also supported the bill. The administration is on board. The agencies that battle these fires are waiting for the Congress to act.

Each day, the reality in the West is that immensely brave men and women are on the ground fighting fires, and they risk their lives to keep our homes and communities protected. It is long, long, long past time for the Congress to step up, fix this budgetary mess, and guarantee that the funding is there to fight fires and to prevent them in the first place.

I filed our bipartisan bill as an amendment to the Transportation bill. I filed a wildfire amendment to the budget resolution. I filed the Senate Interior appropriations wildfire language as an amendment to the Transportation bill. And I believe this is the fourth time in recent months I have been on the floor talking about this issue, and that is in addition to talking about it in the budget markup and in several hearings in the natural resources committee that I had the honor to chair in the last Congress.

I see my new colleague in the chair, and he has been doing good work on this fire borrowing issue. And even with everything else we are dealing with here in the Senate, I think it is very important that we focus on an actual way to leave with an agreement on how this is actually going to get fixed and get done. In that regard, I have been talking in the last day or so with colleagues in both political parties, and I think there is now this sense of urgency because we see it not only on TV, but every time we are home, we go to fire briefings. As the Presiding Officer knows, even fire briefings have changed very dramatically. We used to have a fire briefing in July, and now we have fire briefings—as I did—in the winter because the Forest Service and the folks at BLM often say they are not even sure when one fire season has ended and the next one has begun because these challenges have gotten so great.

Senator CRAPO and I, with this bill that has gotten more than 250 organizations sponsoring it, have talked in just the last few hours. We want to work with all of our colleagues to make sure that we get some sense because our constituents are going to ask about this. They are going to ask about this issue this summer. They are going to ask: How is the Senate actually going to get this done? How is the Senate going to fix this broken, dysfunctional system of fighting fires? In effect, year after year—and I gather there will be some new analyses coming out—the entire budget for the Forest Service is getting eaten up in fighting these counterproductive fires.

Senator CRAPO and I have a proposal that received a favorable score from the Budget Committee. I know my colleague in the chair has also done very good work on these issues, as have a number of Senators on both sides of the aisle. Given the good will I have seen among Senators here in the last couple of days as we talked about what this really means, given the urgency and because we are going home and seeing constituents in August, I am convinced we can have an agreement on how this is going to get fixed. That is why I wanted to come to the floor tonight, because there are a lot of topics that are still going to be tackled in the next few days before the Senate wraps up. I want it understood that our part of the country is on fire. It is on fire. We have communities burning up, and business as usual is unacceptable.

Senator CRAPO and I have offered a proposal that we think will turn this around, and other colleagues have very good ideas as well. What is nonnegotiable is just saying: Oh, you know, maybe we will take care of it at the end of the year or on standard congressional time. That is not good enough for the West, which is burning up.

I invite my colleagues here, as we move forward in the last few days before the August recess, to join me, Senator CRAPO, and colleagues in both political parties to make sure that people see—as we go home to talk to the people we have the honor to represent—that this is now going to actually get fixed and that the Senate is coming together to make sure it actually gets done. We are going to turn this around so that we can do more to prevent fires in the rural west, No. 1, and No. 2, fight them in a more cost-effective way.

With that, I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER (Mr. DAINES). The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

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

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

MORNING BUSINESS

Mr. ROUNDS. Mr. President, I ask unanimous consent that the Senate be in a period of morning business, with Senators permitted to speak therein for up to 10 minutes each.

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

TRIBUTE TO SCOTT WATTS

Mr. REID. Mr. President, I rise today to recognize the distinguished career of Scott ''Scotty'' Watts, who served as the president of the Nevada Alliance for Retired Americans, NARA, from 2001 until his retirement in 2014.

Building on the work of its predecessor, the Nevada National Council of Senior Citizens, NARA has been at the

forefront of advocating for the interests of retired Nevadans for more than a decade. Scotty Watts, who was the founding president of NARA, led the organization and played a critical role in its progress and success. Under his steadfast leadership, Scotty helped NARA build a powerful grassroots network to support the economic and health programs that are important to retirees throughout Nevada. Today, NARA has grown to include more than 19,330 members and 28 chapters, making it the largest progressive senior citizen organization in the Silver State.

Prior to becoming the president of NARA, Scotty was a leading advocate for retirees and seniors in the Silver State. He served two terms as the president of the Nevada National Council of Senior Citizens. Through his leadership positions in these organizations, he led the effort in our State to protect and strengthen the benefits seniors have earned under Social Security and Medicare and has been a fierce advocate for the Affordable Care Act. I am pleased that this month NARA will honor Scotty during the organization's State convention for his career in dedicated service and advocacy.

I have had the pleasure of meeting with Scotty, and I can say without reservation that Nevada's retirees were fortunate to have him in their corner, fighting on their behalf. I commend Scotty for his service to the Silver State, and I wish him the best in his retirement and future endeavors.

DISCRIMINATION AGAINST DOMINICANS OF HAITIAN DESCENT

Mr. LEAHY. Mr. President, I have traveled to the Dominican Republic and Haiti and am familiar with the history of racial tensions between the population of Haitian migrants and Dominicans of Haitian descent and other citizens of the Dominican Republic. These problems are by no means unique to these two neighboring countries, nor are there easy solutions. In addition to race there is competition for land, social services, and jobs. But while this situation should not be oversimplified, the way the Dominican Government is dealing with it is unfortunate.

In a September 2013 Dominican Constitutional Court ruling the citizenship of more than 200,000 people—mostly Dominicans of Haitian descent—was summarily revoked, and they lost access to education, health care, and other essential social services, as well as their basic rights. Since that ruling the Dominican Government has threatened to enforce strict and prejudicial immigration laws. Many affected residents live under constant fear of deportation, and according to the United Nations nearly 20,000 have already fled the country in the past month, putting the island on the brink of a mass refugee crisis.

By threatening to deport Haitian migrants and Dominicans of Haitian descent, the Dominican Government is on a path that not only disregards fundamental principles of international humanitarian law, but may provoke a reaction that makes the situation worse. Even as we are already seeing the consequences of the threat of mass deportations, following through with such a policy would likely greatly exacerbate tensions in the Dominican Republic and create a regional diplomatic and humanitarian crisis. Haiti, impoverished and still recovering from the devastating 2010 earthquake, does not have the capacity to handle the sudden arrival of thousands of homeless, jobless, Dominicans.

The United States, with 319 million people spread across 50 States is among the most ethnically and racially diverse countries in the world. The challenges this has posed for our own democracy over the past two centuries are well known. We have not always handled these challenges as we should have. I hope the Dominican Government will learn from our experience and recognize the need to reverse course and reaffirm the legal status and rights of these people.

NOMINATION OBJECTION

Mr. GRASSLEY. Mr. President, I intend to object to any unanimous consent request at the present time relating to the nomination of David Malcolm Robinson to be Assistant Secretary for Conflict and Stabilization Operations and Coordinator for Reconstruction and Stabilization.

I will object because the State Department has engaged in unreasonable delay in responding to Judiciary Committee investigations and inquiries. Since June of 2013, the Judiciary Committee has requested a number of documents related to an investigation into Ms. Huma Abedin regarding her possible conflicts of interest created by her simultaneous employment with the State Department and private sector entities. In addition, the Judiciary Committee has inquired about former Secretary Clinton and Ms. Abedin's questionable email practices that may be in violation of Department policy and Federal law. Furthermore, the committee's inquiry also centers on the possible interference of Freedom of Information Act requests by State Department personnel, including Secretary Clinton's former Chief of Staff, Ms. Cheryl Mills. To this day, the committee has not received a complete response. Moreover, the committee recently acquired information that shows the State Department has been in possession of material that would answer some of the Committee's inquiries. Yet, the requested material is still not forthcoming.

This willful lack of cooperation is made more evident by the example of repeated failures by State Department personnel to respond to emails or respond days or weeks later. And in yet another recent committee investigation beginning in June 2015, the State Department has still failed to provide any communication, via email or a phone call, to acknowledge or confirm that they have received a committee letter, despite three emails sent by committee staff.

Not only has the Judiciary Committee experienced unacceptable delays in receiving information, other entities inside and outside of the government have experienced delays as well. The Associated Press sued the State Department over the failure to satisfy repeated document requests under the Freedom of Information Act related to these same issues. One of these requests dates back 5 years ago. Judge Richard Leon of the U.S. District Court for the District of Columbia, the judge responsible for this case, chided the State Department for its failure to produce documents on time, ''Now, any person should be able to review that in one day—one day. Even the least ambitious bureaucrat could do this.''

In total, these actions illustrate a pattern of conduct that clearly demonstrates a lack of cooperation and bad faith in its interaction with Congress. This is unacceptable and cannot continue.

In order to maintain the proper balance of separation of powers and in order for Congress to exercise its proper oversight function, government agencies must respond to inquiries. The State Department apparently believes that it can simply ignore Congress. It is important to note that my objection is not intended to question Mr. Robinson's credentials in any way. However, withholding consent to suspend Senate rules on nominations is one tool a Senator has to incentivize executive agencies to respond to congressional inquiries. Frankly, this should not be necessary, and the nominee is an innocent victim of the State Department's contemptuous failures to respond to congressional inquiries. I urge the State Department to change its ways and if they choose not to, I will be forced to escalate the scope of my intent to object to include unanimous consent requests relating to Foreign Service officer candidates as well.

TRIBUTE TO GENERAL RAYMOND T. ODIERNO, 38TH CHIEF OF STAFF OF THE ARMY

Mr. INHOFE. Mr. President, on behalf of myself and my cochair of the Army Caucus, the senior Senator from Rhode Island, Mr. REED, I rise today to honor GEN Raymond T. Odierno, the 38th Chief of Staff of the U.S. Army, and one of our Nation's finest military officers. General Odierno will retire from Active military duty in August 2015, bringing to a close 39 years of distinguished service to our great Nation.

In 1976, General Odierno was commissioned as a second lieutenant in the Field Artillery upon graduation from the United States Military Academy at West Point. He commanded units at

every echelon, from platoon to theater, with duty in Germany, Albania, Kuwait, Iraq, and the United States. General Odierno deployed in support of Operations Desert Shield and Desert Storm; commanded the 4th Infantry Division during Operation Iraqi Freedom from April 2003 to March 2004; served as the commanding general, Multi-National Corps—Iraq, III Corps, from 2006 to 2008; and later served as the commanding general, Multi-National Force—Iraq and subsequently United States Forces—Iraq, from 2008 until 2010. General Odierno went on to serve as the commander of U.S. Joint Forces Command from 2010 to 2011, where he led the development and integration of joint capabilities in support of combatant command requirements around the world.,

On September 7, 2011, General Odierno became the 38th Chief of Staff of the U.S. Army. Since assuming this position, General Odierno's leadership and commitment to his soldiers, to the Army, and to the Nation have significantly contributed to the U.S. Army being the most highly trained and professional land force in the world.

General Odierno developed and implemented the U.S. Army's vision establishing a path for the Army of 2025 and beyond. He envisioned how future Army forces would prevent conflict, shape security environments, and win wars. He ensured that we possessed the capability and capacity to provide globally responsive and regionally aligned forces, as well as expeditionary and decisive land-power across the range of military operations in defense of our Nation at home and abroad, both today and against emerging threats.

But the one thing that remained constant was General Odierno's tireless commitment to soldiers and their families. He built leaders capable of navigating the complex challenges of the world we face today and cared for our families by focusing on keeping the total Army—soldiers, families, and civilians alike—healthy, ready, resilient, and total Army strong. General Odierno is an exceptional leader, an American patriot committed to our Army and Nation, but most importantly, General Odierno is a great man of character. It is for GEN Ray Odierno, a soldier, leader, and selfless servant, whom we with profound admiration and deep respect pay tribute to for all he has done for the U.S. Army and our Nation. We thank General Odierno, his wife Linda, and his three children, Tony, Katie, and Mike, for their dedication and sacrifice, and we wish them well in the years to come.

RECOGNIZING LARRY AND MARGO BEAN

Mr. BARRASSO. Mr. President, on September 1, 2015, the Boys & Girls Club of Central Wyoming will be holding their Annual Awards and Recognition Breakfast where they will honor Casper philanthropists, Larry and Margo Bean.

The Boys & Girls Club of Central Wyoming has been making positive differences in the lives of our children since 1978. The club provides a supportive environment and an extensive array of programs and services to enhance the development of our youth. Through entertaining activities and with the guidance of volunteer mentors, participants learn the important values of independence, community, and belonging. Every year, the Boys & Girls Club plans a breakfast to honor a member or members of the community who make outstanding contributions to both the Boys & Girls Club and the city of Casper. This year's honorees, Larry and Margo Bean, are incredible champions in the Casper community and worthy of this special recognition.

Growing up on farms in Iowa, Larry and Margo moved to Casper as young adults with a desire to help, encourage, and bring joy to those who crossed their paths, particularly children. Anyone who knows the couple knows that the care and support they show for each other equals their passion for philanthropy and civic engagement. Next year, the couple will celebrate their 50th anniversary. They will celebrate this milestone occasion with their children Joshua, Amber, Nathan, and Nicole, and grandchildren Ella, Xavier, Mia, Mars, Sullivan, Cassius, and Vincent—who will be born next month.

As a couple, they are a powerhouse, yet they have significant individual accomplishments. As an author of four children's books, Margo's inspiration to write stories for children came from her father, Max Cronbaugh. Her father was an amazing storyteller who never failed to capture the imagination of children and the excitement of everyday life on the farm. With her experience as an elementary school teacher and growing up on her family's Iowa farm, Margo's books reflect her unique experience and the special place children have always held in her heart. Her continued dedication to educating children in Wyoming is shown by leadership efforts at the St. Anthony Tri-Parish Catholic School, where some of their grandchildren attend school. Additionally, Margo was chairman of the Wyoming Medical Center board of directors and ran a successful business.

Larry is a certified public accountant and he provides valuable guidance and financial advice. In addition, Larry serves on the board of directors for several important organizations including the Martin Family Foundation, the Converse County Bank, and the Central Wyoming Counseling Center. As so many folks in Wyoming know, Larry is the ultimate letterwriter. His letters are individual masterpieces. In every letter from Larry, you see his smile and feel his friendship. Larry freely gives encouragement and inspiration—one letter at a time. Over the years, Bobbi and I have looked forward to the Bean's annual Christmas letter.

Together, Larry and Margo have touched the lives of thousands of children and families in Wyoming through their philanthropic and volunteer work. At Christmastime, their ''Love in Action'' project collects presents for families in need. They sponsor and coordinate youth events in the community including The American Dream Essay contest, The Uprising, and the Global Leadership Summit. The Beans also support youth faith-based organizations such as Child Evangelism Fellowship and Youth for Christ. They also have been strong supporters of the Nicolaysen Discovery Center and the Central Wyoming Rescue Mission.

Their kindness and generosity expands across the globe. Larry and Margo are diligently working to develop faith-based schools in Zambia and Haiti. These neighborhood schools will bring hope and opportunities to these children as well as to these communities.

My wife, Bobbi, joins me in extending our congratulations to Larry and Margo Bean and thanking them for their dedication to Wyoming and its youth. All of us privileged to know them are blessed.

ADDITIONAL STATEMENTS

VANDERBILT UNIVERSITY WOMEN'S TENNIS TEAM NATIONAL CHAMPIONSHIP

• Mr. ALEXANDER. Mr. President, as a fellow Commodore, I would like to congratulate the Vanderbilt University women's tennis team on winning the NCAA championship, the first national championship for the women's tennis program, and the third in Commodore history.

Geoff Macdonald, the head coach of this program for 21 years, has done a phenomenal job of training and guiding these exceptional student-athletes. He has worked hard to transform the Vanderbilt's women's tennis program into the best in the country.

Vanderbilt is a very special university, one that produces student-athletes of exceptional character and integrity, who have pride in themselves and their school. This may be the first national championship for Vanderbilt's women's tennis team, but their commitment to these ideals ensures that this success will not be the last.

This achievement would not have been possible without the hard work, talent, and teamwork of the following outstanding student-athletes: Payton Robinette, Margaret Leavell, Ellie Yates, Georgina Sellyn, Ashleigh Antal, Marie Casares, Courtney Colton, Frances Altick, Astra Sharma, and Sydney Campbell.

Of course, these student-athletes were trained and mentored by a dedicated team of coaches and staff led by Coach Macdonald. They are: Emil Iankov, Christy Hogan, Kerry Wilbar, Lori Alexander, Aleke Tsoubanos, and Catherine Hilley.

Go 'Dores!•

CONCORD, NEW HAMPSHIRE 250TH ANNIVERSARY

• Ms. AYOTTE. Mr. President, I rise today in honor of Concord, NH—a city in Merrimack County that is celebrating the 250th anniversary of its founding. I am proud to join the citizens across the Granite State in recognizing this special occasion.

Concord, settled in 1725 by colonists from Massachusetts, was incorporated in 1733 as the town of Rumford, and later the parish of Concord where it experienced several border disputes with the neighboring town of Bow. The parish of Bow officially became part of Concord in 1765.

Concord includes the villages of Penacook, East Concord, and West Concord. The city's population has grown to over 40,000 residents with over 6,000 acres of protected land. Concord residents have access to numerous hiking and biking trails, and the town's location on the Merrimack River significantly adds to its natural beauty.

In 1808, Concord was established as the State capital of New Hampshire. The statehouse is the oldest legislative building in the Nation still in use by the State's house and senate. The house chamber is also home to the largest State legislative body in the country.

Concord has produced many innovative businesses, including the Abbot-Downing Company that designed and built the world-famous Concord Coach in 1827, revolutionizing travel throughout the world.

Today, Concord is a civic, cultural, business, and medical hub for the Granite State. It is where New Hampshire's lone U.S. President, Franklin Pierce had an office, and it is the location of his final resting place. Concord is also home to the McAuliffe-Shepard Discovery Center, named after Christa McAuliffe, a Concord educator who bravely volunteered to become the first teacher in space aboard the fatal Challenger space shuttle mission in 1986, and New Hampshire astronaut Alan Shepard. Today, new generations can visit the planetarium to learn about our universe. On Concord's thriving Main Street, residents and visitors can find an outstanding collection of New Hampshire small businesses that represent the heart of the city. Downtown Concord is full of history and culture—including the Museum of New Hampshire History, the Capital Center for the Arts, and the Red River Theater.

The spirit of community and volunteerism is strong in Concord as evidenced by the hard work and dedication of all involved with the planning and celebration of this special sestercentennial anniversary.

Concord, as our State's capital, has greatly contributed to the life and spirit of New Hampshire. I am pleased to extend my warm regards to the people of Concord as they celebrate the city's 250th anniversary.•

PITTSBURG, NEW HAMPSHIRE 175TH ANNIVERSARY

• Ms. AYOTTE. Mr. President, today I wish to pay tribute to Pittsburg, NH—a town in Coos County that is celebrating the 175th anniversary of its founding. I am proud to join citizens across the Granite State in recognizing this historic occasion.

Pittsburg is nestled deep within New Hampshire's Great North Woods and sits in the shadows of Stub Hill and Magalloway Mountain. It is the largest town by area in the State, and contains all four Connecticut Lakes. Pittsburg is the only town that shares a border with both Maine and Vermont, and contains the only portion of New Hampshire west of the Connecticut River. Pittsburg holds the only New Hampshire crossing into Canada, sharing an international border with the Province of Québec.

The area known as Pittsburg was settled in the early part of the 19th century, but an unclear boundary line between the United States and Canada allowed for the formation of a region known as the Republic of Indian Stream. Shortly thereafter, the town was incorporated in 1840 and named for English Prime Minister William Pitt.

Pittsburg is home to scenic lakes, rivers, streams, and forestland, and has become the perfect venue for all recreational outdoor activities. Thousands of off-highway recreational vehicle enthusiasts visit each season to enjoy the hundreds of miles of snowmobile and ATV trails that have earned Pittsburg the title, ''snowmobile capital of New England.''

On behalf of all Granite Staters, I am pleased to offer my congratulations to the residents of Pittsburg on reaching this special milestone, and I thank them for their many contributions to the life and spirit of the State of New Hampshire.•

REMEMBERING LOIS HORVITZ

• Mrs. BOXER. Mr. President, I ask my colleagues to join me in honoring the life of Lois Horvitz, a beloved mother, grandmother, public health advocate, and extraordinary philanthropist who passed away on July 23, 2015. She was 88 years old.

Lois Horvitz was born April 22, 1927 in Cleveland, OH. She attended the University of Wisconsin before marrying Harry R. Horvitz, a World War II naval officer and newspaper publisher.

In 1962, Lois met Dr. Claude S. Beck, a renowned cardiac surgeon and pioneer of cardiopulmonary resuscitation, the lifesaving technique more commonly known as CPR. Inspired by his work, Lois became an early advocate of CPR training, championing a wide spread public awareness campaign and establishing the Resuscitators of America to teach CPR classes.

Lois' efforts to promote CPR awareness sparked her lifelong passion for philanthropy, inspiring her to dedicate her time and resources to improving lives in her community and country. In addition to serving on the boards of the Eisenhower Medical Center and the Betty Ford Center, Lois established the Harry R. Horvitz Center for Palliative Medicine at the Cleveland Clinic in honor of her late husband of 44 years. An active member of her Indian Wells community, Lois created the Desert Town Hall in 1993, which became an annual speaker series featuring world leaders.

I send my deepest condolences to Lois' children, Michael, Pam, and Peter, and their families. Lois' legacy of commitment and compassion will continue to inspire others for years to come.•

REMEMBERING SERGEANT SCOTT LUNGER

• Mrs. BOXER. Mr. President, today I ask my colleagues to join me in paying tribute to Sergeant Scott Lunger, an exceptional law enforcement officer, loyal friend, and beloved father who was tragically killed in the line of duty on July 22, 2015.

Scott Lunger was born on March 13, 1967 and grew up in Dublin, CA, where he played baseball and football at Dublin High School. After graduation, Scott followed his father and older brother's footsteps and entered the electrical trade, becoming a member of IBEW Local 595. However, a lifelong interest in law enforcement prompted Scott to switch career paths, and he began working as a Contra Costa County sheriff's deputy before transferring to the Hayward Police Department in 2001.

During his 15-year career with the department, Sergeant Lunger was assigned to some of the most critical units, including the gang task force, SWAT team, and the special duty unit. Sergeant Lunger also worked as a field training officer and became the head of the field training unit, allowing him to mentor dozens of young officers on the force. Sergeant Lunger's colleagues recalled admiringly his ability to encourage his fellow officers to give their best effort, always leading by example.

Sergeant Lunger dedicated his life to his family, his community, and his country. On behalf of the people of California, whom he served so bravely, I extend my gratitude and deepest sympathies to his daughters, Ashton and Saralyn; father, Paul; brothers, Mike and Todd; sisters, Michelle and Ciara; nieces and nephews; and entire extended family. His dedicated and courageous service will never be forgotten.•

REMEMBERING JOSEPH MENDOZA, JR.

• Mrs. BOXER. Mr. President, today I ask my colleagues to join me in honoring the life of my good friend, Joey Mendoza, a longtime pillar of the West Marin ranching community.

Born in 1943, Joey grew up on his family's historic B Ranch in Point Reyes National Seashore, which had been purchased by his grandfather in 1919. After attending college at Cal Poly, San Luis Obispo, Joey returned to Marin County to work in the family business, becoming a third-generation dairyman.

I first met Joey during my time as a Marin County supervisor, and although we did not see eye to eye on every issue, Joey was always willing to work together to try to forge consensus. He never let political differences get in the way of personal relationships, and over the years we formed an unwavering friendship.

A well-respected and beloved member of the Marin community, Joey gave generously of his time and energy to numerous organizations throughout his career, including the Western United Dairymen and the Marin County Farm Bureau. A lifelong farming advocate, Joey worked tirelessly to preserve California's North Bay agricultural heritage. It is a testament to his lifelong passion that his children decided to follow in their father's footsteps by operating their own ranches, with Joey's son maintaining the family's operation at B Ranch nearly 100 years after his great-grandfather worked the land. Joey and his family's legacy will help ensure that ranching and dairy operations will be part of the fabric of the Marin community for generations to come.

With his warm and welcoming nature, Joey remained a leading voice for the ranching community until his final days. I send my deepest condolences to Joey's wife Linda, his son Jarrod, his daughter Jolynn, his brother Jim, and his grandchildren, Collin, Luke, and Layla, along with his entire extended family.●

REMEMBERING OFFICER DAVID JOSEPH NELSON

● Mrs. BOXER. Mr. President, I ask my colleagues to join me in honoring the life of Bakersfield Police Officer David Joseph Nelson, a beloved son, brother, and grandson who was tragically killed in the line of duty on June 26, 2015.

David Nelson was born on November 16, 1988 in Burbank, CA. He graduated with top honors from Burbank High School in 2007, where he was a member of the Associated Student Body and the varsity swim and water polo teams. Officer Nelson attended Occidental College, earning a bachelor's degree in economics with a minor in public policy. He was also a member of Occidental's water polo and basketball teams.

As a college student, Officer Nelson interned with the U.S. Department of the Treasury and was offered a position upon graduation. However, he chose to remain in California to follow his lifelong dream of pursuing a career in law enforcement. In 2008, he joined the Burbank Police Department as a police cadet and became an officer with the Bakersfield Police Department in 2013.

At a memorial service on July 1, 2015, Bakersfield Police Sergeant Uriel Pacheco recalled that Officer Nelson was a ''dedicated, trustworthy, courageous and respectful'' member of the department. Others remembered David Nelson as a talented athlete with a great sense of humor and a strong desire to help those less fortunate.

On behalf of the people of California, whom Officer Nelson served so bravely, I extend my deepest sympathy to his parents Larry and Mary, brothers Erik and Michael, grandmothers Elsie Nelson and Josephine Gutierrez, and many uncles, aunts, cousins and friends.

We are forever indebted to Officer David Joseph Nelson for his courage and sacrifice, and he will be deeply missed.●

CONGRATULATING LIEUTENANT GENERAL BRUCE A. LITCHFIELD

● Mr. INHOFE. Mr. President, today on behalf of Senator LANKFORD and myself, we are pleased to congratulate Lt. Gen. Bruce A. Litchfield upon the completion of his career of service in the U.S. Air Force. Throughout his 34-year military career, Lieutenant General Litchfield served with distinction and dedication, ultimately becoming the commander of the Air Force Sustainment Center at Tinker Air Force Base, OK, responsible for providing operational planning and execution of Air Force Supply Chain Management and Depot Maintenance for a wide range of aircraft, engines, missiles, and component items in support of Air Force Materiel Command missions. From his command in Oklahoma, he was responsible for operations which spanned 3 air logistics complexes, 3 air base wings, 2 supply chain management wings, and multiple remote operating locations, incorporating more than 32,000 military and civilian personnel. Finally, he oversaw installation support to more than 75,000 personnel working in 140 associate units at the 3 sustainment center bases.

In July 2012, General Litchfield became the first commander of the newly established Air Force Sustainment Center in Oklahoma. During his command, he returned over $1.5 billion back to the Air Force, and ultimately the taxpayer, through comprehensive initiatives like the AFSC Way and Cost Effective Readiness.

General Litchfield entered the Air Force in 1981 as a distinguished graduate from the Reserve Officer Training Corps program at Norwich University in Vermont. During his distinguished career, Lieutenant General Litchfield commanded at the squadron and group levels in addition to commanding two wings, and was the director of logistics, Headquarters Pacific Air Forces, Hickam Air Force Base, Hawaii. He spent the last 6 years in the great State of Oklahoma at Tinker Air Force Base as commander of the Oklahoma City Air Logistics Center, as well as commander of the Air Force Sustainment Center.

General Litchfield earned military awards to include the Defense Service Medal, Legion of Merit with two oak leaf clusters, Defense Meritorious Service Medal, Meritorious Service Medal with four oak leaf clusters, the Air Force Commendation Medal, and the Air Force Achievement Medal as well as other service awards.

Under General Litchfield's command, the Air Force Sustainment Center earned two of the prestigious Department of Defense Maintenance Effectiveness Awards, as well as the Outstanding Unit Award.

General Litchfield led the successful reorganization and standup of the Air Force Sustainment Center, placing command and control of depot maintenance, supply chain and associate air base wing support under one command chain of command at Tinker Air Force Base, OK. His proactive leadership incorporated a revolutionary leadership model and governance process that drove rapid culture change and is currently under review by multiple universities as the example of success for government and industry.

General Litchfield, his wife Linda, and children Matthew and Jennifer have made many sacrifices during his Air Force career, and we appreciate their contributions of conscientious service to our country. His family and his fellow airmen can be proud of his service.

As he departs the Air Force to start the next part of his journey, I call upon my colleagues to wish Bruce and his family every success. It is our pleasure to recognize him at the conclusion of a distinguished career of service to the Air Force and to the United States of America.●

RECOGNIZING COCO EROS

● Mr. VITTER. Mr. President, in the wake of the recent tragedy in Lafayette, I wish to recognize Coco Eros Clothing Boutique and Design Studio as Small Business of the Week for their efforts in supporting the Lafayette community. Small businesses are created by entrepreneurs who not only have a passion for their companies, but also have love for their community members.

In the days after the July 23, 2015, shooting at the Grand 16 Movie Theater in Lafayette, LA, Coco Eros sought to support the victims' recovery and families by selling a necklace designed by Mayci Breaux, who lost her life in the tragic attack. Mayci was an employee at Coco Eros and was preparing for a career as an ultrasound and radiology technician. The proceeds of her design—the Mayci necklace—will go to the families of the victims. It is my honor to recognize the thoughtfulness of the folks at Coco Eros through this week's Small Business of the Week.

Coco Eros was founded in 2009 by fashion enthusiasts Monica Broussard

and Emily Adams, whose goal is to share their love for clothing and accessories with local customers. The locally owned and operated boutique prides itself on its friendly and personable shopping experience. With a sofa to lounge on and helpful staff on hand, the store is a community staple contributing unique and trending fashion and accessories. Monica and Emily focus on fashion-forward clientele, carefully selecting trend-conscious labels and styles. Coco Eros features popular, contemporary clothing lines like Trina Turk, Paige, La Bella Vita, and Joie. The store provides in-store alteration services, and co-owner Emily designs and creates original, customized dresses. Monica and Emily take advantage of social media opportunities as well, with popular Facebook and Instagram accounts that feature Emily's original designs and happy, well-dressed customers. At Coco Eros, the goal is to promote good style and self-confidence for each customer.

Congratulations again to Coco Eros for being selected as Small Business of the Week. We appreciate your thoughtful contributions to the Lafayette community.●

RECOGNIZING RED ARROW WORKSHOP

● Mr. VITTER. Mr. President, in the wake of the recent tragedy in Lafayette, I wish to recognize Red Arrow Workshop as Small Business of the Week in memory of co-owner Jillian Johnson, who lost her life in the July 23, 2015, shooting at The Grand 16 Movie Theater in Lafayette, LA.

Jillian Johnson and her husband Jason Brown spent years ''planning, plotting, and scheming'' before opening Red Arrow Workshop in August 2012. Jillian was well-known for her creativity, kindness, and generosity, which translated directly into the success of her family-owned small business. Red Arrow Workshop is a locally owned-and-operated gift, apparel, accessories, and toy shop showcasing a variety of products unavailable anywhere else in Acadiana. The shop also showcases the local, specialty t-shirt line Parish Ink—of which Jillian was a creative partner. After 2 successful years in Lafayette, she and Jason expanded their thriving business, opening a second shop on Magazine Street in New Orleans, LA.

Beloved by locals and cited by many as an artistic staple in the community, Red Arrow Workshop hosts a thoughtfully curated, ever-changing collection of American-made, fair-trade, handmade, and eco-friendly items—including products of several talented south Louisiana artists. The shop's Louisiana-themed items are some of their most popular, with artistic representations of the Mississippi River and State silhouettes covering a collection of prints, paintings, stickers, and home goods. Red Arrow also sells a collection of quirky books, fabrics, and paper goods.

It is my honor to designate Red Arrow Workshop as Small Business of the Week. Small businesses are created by entrepreneurs who not only have love for their companies, but also have love for their community members. Jillian and Jason have contributed to the Lafayette community with their earnest and enthusiastic entrepreneurial spirit. Together we are all ''Lafayette Strong.''●

MESSAGE FROM THE HOUSE

At 12:43 p.m., a message from the House of Representatives, delivered by Mr. Novotny, one of its reading clerks, announced that the House has agreed to the following concurrent resolution, in which it requests the concurrence of the Senate:

H. Con. Res. 72. Concurrent resolution providing for a conditional adjournment of the House of Representatives and a conditional recess or adjournment of the Senate.

EXECUTIVE AND OTHER COMMUNICATIONS

The following communications were laid before the Senate, together with accompanying papers, reports, and documents, and were referred as indicated:

EC–2464. A communication from the Director of the Regulatory Management Division, Environmental Protection Agency, transmitting, pursuant to law, the report of a rule entitled ''Fluazifop-P-butyl; Pesticide Tolerance'' (FRL No. 9930–99) received during adjournment of the Senate in the Office of the President of the Senate on July 31, 2015; to the Committee on Agriculture, Nutrition, and Forestry.

EC–2465. A communication from the Associate General Counsel, Office of the General Counsel, Department of Agriculture, transmitting, pursuant to law, a report relative to a vacancy in the position of General Counsel, Department of Agriculture, received in the Office of the President of the Senate on August 3, 2015; to the Committee on Agriculture, Nutrition, and Forestry.

EC–2466. A communication from the Secretary of Education, transmitting, pursuant to law, a report of a violation of the Antideficiency Act within the Program Administration, Departmental Management, Education account; to the Committee on Appropriations.

EC–2467. A communication from the Assistant Director, Senior Executive Management Office, Department of Defense, transmitting, pursuant to law, a report relative to a vacancy in the position of Under Secretary of the Army, Department of the Army, received in the Office of the President of the Senate on July 29, 2015; to the Committee on Armed Services.

EC–2468. A communication from the Assistant Director, Senior Executive Management Office, Department of Defense, transmitting, pursuant to law, a report relative to a vacancy in the position of Under Secretary of Defense (Personnel and Readiness), Department of Defense, received in the Office of the President of the Senate on July 29, 2015; to the Committee on Armed Services.

EC–2469. A communication from the Assistant Director, Senior Executive Management Office, Department of Defense, transmitting, pursuant to law, a report relative to a vacancy in the position of Department of Defense General Counsel, Department of Defense, received in the Office of the President of the Senate on July 29, 2015; to the Committee on Armed Services.

EC–2470. A communication from the Under Secretary of Defense (Personnel and Readiness), transmitting a report on the approved retirement of Lieutenant General John D. Johnson, United States Army, and his advancement to the grade of lieutenant general on the retired list; to the Committee on Armed Services.

EC–2471. A communication from the Assistant Secretary for Export Administration, Bureau of Industry and Security, Department of Commerce, transmitting, pursuant to law, the report of a rule entitled ''U.S. Industrial Base Surveys Pursuant to the Defense Production Act of 1950'' (RIN0694–AG17) received in the Office of the President of the Senate on July 22, 2015; to the Committee on Banking, Housing, and Urban Affairs.

EC–2472. A communication from the Chief Counsel, Federal Emergency Management Agency, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Suspension of Community Eligibility'' ((44 CFR Part 64) (Docket No. FEMA–2015–0001)) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Banking, Housing, and Urban Affairs.

EC–2473. A communication from the Assistant Secretary for Export Administration, Bureau of Industry and Security, Department of Commerce, transmitting, pursuant to law, the report of a rule entitled ''Cuba: Implementing Rescission of State Sponsor of Terrorism Designation'' (RIN0694–AG60) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Banking, Housing, and Urban Affairs.

EC–2474. A communication from the Director of Legislative Affairs, Federal Deposit Insurance Corporation, transmitting, pursuant to law, the report of a rule entitled ''Regulatory Capital Rules: Regulatory Capital, Final Revisions Applicable to Banking Organizations Subject to the Advanced Approaches Risk-Based Capital Rule'' (RIN3064–AE12) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Banking, Housing, and Urban Affairs.

EC–2475. A communication from the General Counsel of the Federal Housing Finance Agency, transmitting, pursuant to law, the report of a rule entitled ''Organization and Functions, and Seal Amendments'' (RIN2590–AA75) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Banking, Housing, and Urban Affairs.

EC–2476. A communication from the General Counsel of the National Credit Union Administration, transmitting, pursuant to law, the report of a rule entitled ''Loans in Areas Having Special Flood Hazards'' (RIN3133–AE40) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Banking, Housing, and Urban Affairs.

EC–2477. A communication from the Assistant Secretary for Export Administration, Bureau of Industry and Security, Department of Commerce, transmitting, pursuant to law, the report of a rule entitled ''Addition of Certain Persons to the Entity List; and Removal of Certain Persons from the Entity List Based on Removal Requests'' (RIN0694–AG61) received during adjournment of the Senate in the Office of the President of the Senate on July 31, 2015; to the Committee on Banking, Housing, and Urban Affairs.

EC–2478. A communication from the Assistant General Counsel, General Law, Ethics, and Regulation, Department of the Treasury, transmitting, pursuant to law, a report relative to a vacancy in the position of Director

of the Mint, Department of the Treasury, received in the Office of the President of the Senate on July 30, 2015; to the Committee on Banking, Housing, and Urban Affairs.

EC–2479. A communication from the Assistant General Counsel for Legislation, Regulation and Energy Efficiency, Office of Energy Efficiency and Renewable Energy, Department of Energy, transmitting, pursuant to law, the report of a rule entitled ''Energy Conservation Program: Test Procedure for Refrigerated Bottled or Canned Beverage Vending Machines'' ((RIN1904–AD07) (Docket No. EERE–2013–BT–TP–0045)) received during adjournment of the Senate in the Office of the President of the Senate on July 31, 2015; to the Committee on Energy and Natural Resources.

EC–2480. A communication from the Assistant General Counsel for Legislation, Regulation and Energy Efficiency, Office of Energy Efficiency and Renewable Energy, Department of Energy, transmitting, pursuant to law, the report of a rule entitled ''Energy Conservation Program: Test Procedures for Dehumidifiers'' ((RIN1904–AC80) (Docket No. EERE–2014–BT–TP–0010)) received during adjournment of the Senate in the Office of the President of the Senate on July 31, 2015; to the Committee on Energy and Natural Resources.

EC–2481. A communication from the General Counsel, Federal Energy Regulatory Commission, transmitting, pursuant to law, the report of a rule entitled ''Revisions to Public Utility Filing Requirements'' (Docket No. RM15–3–000) received during adjournment of the Senate in the Office of the President of the Senate on July 31, 2015; to the Committee on Energy and Natural Resources.

EC–2482. A communication from the Director of the Regulatory Management Division, Environmental Protection Agency, transmitting, pursuant to law, the report of a rule entitled ''Approval and Promulgation of Air Quality Implementation Plans; Pennsylvania; Infrastructure Requirements for the 2008 Ozone and 2010 Sulfur Dioxide National Ambient Air Quality Standards'' (FRL No. 9931–80–Region 3) received during adjournment of the Senate in the Office of the President of the Senate on July 31, 2015; to the Committee on Environment and Public Works.

EC–2483. A communication from the Director of the Regulatory Management Division, Environmental Protection Agency, transmitting, pursuant to law, the report of a rule entitled ''Approval and Promulgation of Air Quality Implementation Plans; Missouri; Update to Materials Incorporated by Reference'' (FRL No. 9927–41–Region 7) received during adjournment of the Senate in the Office of the President of the Senate on July 31, 2015; to the Committee on Environment and Public Works.

EC–2484. A communication from the Director of the Regulatory Management Division, Environmental Protection Agency, transmitting, pursuant to law, the report of a rule entitled ''Approval and Promulgation of Air Quality Implementation Plans; Maryland; Amendments to the Control of Gasoline and Volatile Organic Compound Storage and Handling'' (FRL No. 9931–54–Region 3) received during adjournment of the Senate in the Office of the President of the Senate on July 31, 2015; to the Committee on Environment and Public Works.

EC–2485. A communication from the Director of the Regulatory Management Division, Environmental Protection Agency, transmitting, pursuant to law, the report of a rule entitled ''Approval and Promulgation of Air Quality Implementation Plans; Connecticut; Approval of NOx Emission Offset Credits as Single Source SIP Revisions'' (FRL No. 9927–49–Region 1) received during adjournment of the Senate in the Office of the President of the Senate on July 31, 2015; to the Committee on Environment and Public Works.

EC–2486. A communication from the Assistant Secretary for Legislation, Department of Health and Human Services, transmitting, pursuant to law, a report entitled ''Assessing the Continued Suspension of the Long Term Care Hospital (LTCH) 25 Percent Policy''; to the Committee on Finance.

EC–2487. A communication from the Chief of the Publications and Regulations Branch, Internal Revenue Service, Department of the Treasury, transmitting, pursuant to law, the report of a rule entitled ''Expatriate Health Coverage Clarification Act of 2014, Interim Guidance'' (Notice 2015–43) received during adjournment of the Senate in the Office of the President of the Senate on July 31, 2015; to the Committee on Finance.

EC–2488. A communication from the Chief of the Publications and Regulations Branch, Internal Revenue Service, Department of the Treasury, transmitting, pursuant to law, the report of a rule entitled ''Safe Harbor for Ratable Service Contracts'' (Rev. Proc. 2015–39) received during adjournment of the Senate in the Office of the President of the Senate on July 31, 2015; to the Committee on Finance.

EC–2489. A communication from the Deputy Director, Centers for Medicare and Medicaid Services, Department of Health and Human Services, transmitting, pursuant to law, the report of a rule entitled ''Medicare Program; Inpatient Psychiatric Facilities Prospective Payment System—Update for Fiscal Year Beginning October 1, 2015 (FY 2016)'' ((RIN0938–AS47) (CMS–1627-F)) received in the Office of the President of the Senate on August 3, 2015; to the Committee on Finance.

EC–2490. A communication from the Deputy Director, Centers for Medicare and Medicaid Services, Department of Health and Human Services, transmitting, pursuant to law, the report of a rule entitled ''Medicare Program; Prospective Payment System and Consolidated Billing for Skilled Nursing Facilities (SNFs) for FY 2016, SNF Value-Based Purchasing Program, SNF Quality Reporting Program, and Staffing Data Collection'' ((RIN0938–AS44) (CMS–1622-F)) received in the Office of the President of the Senate on August 3, 2015; to the Committee on Finance.

EC–2491. A communication from the Deputy Director, Centers for Medicare and Medicaid Services, Department of Health and Human Services, transmitting, pursuant to law, the report of a rule entitled ''Medicare Program; FY 2016 Hospice Wage Index and Payment Rate Update and Hospice Quality Reporting Requirements'' ((RIN0938–AS39) (CMS–1629-F)) received in the Office of the President of the Senate on August 3, 2015; to the Committee on Finance.

EC–2492. A communication from the Deputy Director, Centers for Medicare and Medicaid Services, Department of Health and Human Services, transmitting, pursuant to law, the report of a rule entitled ''Medicare Program; Hospital Inpatient Prospective Payment Systems . . . Payment Adjustment for Hospitals'' ((RIN0938–AS41) (CMS–1632-F and IFC)) received in the Office of the President of the Senate on August 3, 2015; to the Committee on Finance.

EC–2493. A communication from the Deputy Director, Centers for Medicare and Medicaid Services, Department of Health and Human Services, transmitting, pursuant to law, the report of a rule entitled ''Medicare Program; Inpatient Rehabilitation Facility Prospective Payment System for Federal Fiscal Year 2016'' ((RIN0938–AS45) (CMS–1624-F)) received in the Office of the President of the Senate on August 3, 2015; to the Committee on Finance.

EC–2494. A communication from the Acting Assistant Secretary, Bureau of Political-Military Affairs, Department of State, transmitting, pursuant to law, an addendum to a certification of the proposed sale or export of defense articles and/or defense services to a Middle East country (OSS–2015–1237); to the Committee on Foreign Relations.

EC–2495. A communication from the Assistant Secretary, Legislative Affairs, Department of State, transmitting, pursuant to law, a report relative to section 36(c) of the Arms Export Control Act (DDTC 14–132); to the Committee on Foreign Relations.

EC–2496. A communication from the Assistant Secretary, Bureau of Political-Military Affairs, Department of State, transmitting, pursuant to law, an addendum to a certification of the proposed sale or export of defense articles and/or defense services to a Middle East country (OSS–2015–1241); to the Committee on Foreign Relations.

EC–2497. A communication from the Assistant Secretary, Bureau of Political-Military Affairs, Department of State, transmitting, pursuant to law, an addendum to a certification of the proposed sale or export of defense articles and/or defense services to a Middle East country (OSS–2015–1240); to the Committee on Foreign Relations.

EC–2498. A communication from the Assistant Secretary, Bureau of Political-Military Affairs, Department of State, transmitting, pursuant to law, an addendum to a certification of the proposed sale or export of defense articles and/or defense services to a Middle East country (OSS–2015–1239); to the Committee on Foreign Relations.

EC–2499. A communication from the Acting Assistant Secretary, Bureau of Political-Military Affairs, Department of State, transmitting, pursuant to law, an addendum to a certification of the proposed sale or export of defense articles and/or defense services to a Middle East country (OSS–2015–1238); to the Committee on Foreign Relations.

EC–2500. A communication from the Assistant Secretary, Legislative Affairs, Department of State, transmitting, pursuant to law, a report relative to section 36(c) of the Arms Export Control Act (DDTC 15–035); to the Committee on Foreign Relations.

EC–2501. A communication from the Assistant Secretary, Legislative Affairs, Department of State, transmitting, pursuant to law, a report relative to section 36(c) of the Arms Export Control Act (DDTC 15–043); to the Committee on Foreign Relations.

EC–2502. A communication from the Assistant Secretary, Legislative Affairs, Department of State, transmitting, pursuant to law, a report relative to section 36(c) of the Arms Export Control Act (DDTC 15–065); to the Committee on Foreign Relations.

EC–2503. A communication from the Assistant Secretary for Legislation, Department of Health and Human Services, transmitting, pursuant to law, a report entitled ''Federal Agency Drug-Free Workplace Programs''; to the Committee on Health, Education, Labor, and Pensions.

EC–2504. A communication from the Assistant Secretary for Legislation, Department of Health and Human Services, transmitting, pursuant to law, a report entitled ''2012 Regional Partnership Grants to Increase the Well-Being of and to Improve the Permanency Outcomes for Children Affected by Substance Abuse Second Annual Report to Congress''; to the Committee on Health, Education, Labor, and Pensions.

EC–2505. A communication from the Director, Office of Personnel Management, transmitting, pursuant to law, the Office's fiscal year 2014 annual report relative to the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002; to the Committee on Homeland Security and Governmental Affairs.

EC–2506. A communication from the Director of the Office of Regulatory Affairs and Collaborative Action, Bureau of Indian Affairs, Department of the Interior, transmitting, pursuant to law, the report of a rule entitled ''Federal Acknowledgment of American Indian Tribes'' (RIN1076–AF18) received in the Office of the President of the Senate on July 30, 2015; to the Committee on Indian Affairs.

EC–2507. A communication from the Chair, U.S. Sentencing Commission, transmitting, pursuant to law, a report entitled ''Impact of the Fair Sentencing Act of 2010''; to the Committee on the Judiciary.

EC–2508. A communication from the Acting Deputy Under Secretary of Defense (Personnel and Readiness), transmitting, pursuant to law, the Federal Voting Assistance Program's 2014 Post-Election Survey Report; to the Committee on Rules and Administration.

EC–2509. A communication from the Attorney-Advisor, U.S. Coast Guard, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Safety Zone; The Cleveland Yachting Club Annual Regatta Fireworks Display; Lake Erie, Rocky River, OH'' ((RIN1625–AA00) (Docket No. USCG–2015–0613)) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2510. A communication from the Attorney-Advisor, U.S. Coast Guard, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Safety Zone; Lake Metroparks Stand-Up Paddleboard Race; Lake Erie; Fairport Harbor, OH'' ((RIN1625–AA00) (Docket No. USCG–2015–0612)) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2511. A communication from the Attorney-Advisor, U.S. Coast Guard, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Drawbridge Operation Regulation; Victoria Barge Canal, Bloomington, TX'' ((RIN1625–AA09) (Docket No. USCG–2014–0952)) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2512. A communication from the Attorney-Advisor, U.S. Coast Guard, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Safety Zone; POLAR PIONEER, Outer Continental Shelf Drill Unit, Chukchi Sea, Alaska'' ((RIN1625–AA00) (Docket No. USCG–2015–0247)) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2513. A communication from the Attorney-Advisor, U.S. Coast Guard, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Safety Zones; Misery Challenge, Manchester Bay, Manchester, MA'' ((RIN1625–AA00) (Docket No. USCG–2015–0188)) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2514. A communication from the Attorney-Advisor, U.S. Coast Guard, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Safety Zone; Block Island Wind Farm; Rhode Island Sound, RI'' ((RIN1625–AA00) (Docket No. USCG–2015–0227)) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2515. A communication from the Attorney-Advisor, U.S. Coast Guard, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Special Local Regulation; Southeast Drag Boat Championships, Atlantic Intracoastal Waterway; Buckport, SC'' ((RIN1625–AA08) (Docket No. USCG–2015–0045)) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2516. A communication from the Attorney-Advisor, U.S. Coast Guard, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Special Local Regulation; Beaufort Water Festival, Beaufort, SC'' ((RIN1625–AA08) (Docket No. USCG–2015–0192)) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2517. A communication from the Attorney-Advisor, U.S. Coast Guard, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Special Local Regulation; Mavericks Surf Competition, Half Moon Bay, CA'' ((RIN1625–AA08) (Docket No. USCG–2015–0427)) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2518. A communication from the Attorney-Advisor, U.S. Coast Guard, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Safety Zone; Town of Olcott Fireworks Display; Lake Ontario, Olcott, NY'' ((RIN1625–AA00) (Docket No. USCG–2015–0613)) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2519. A communication from the Attorney-Advisor, U.S. Coast Guard, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Safety Zones and Regulated Navigation Area; Shell Arctic Drilling/Exploration Vessels and Associated Voluntary First Amendment Area, Puget Sound, WA, Extension'' ((RIN1625–AA00 and RIN1625–AA11) (Docket No. USCG–2015–0295)) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2520. A communication from the Attorney-Advisor, U.S. Coast Guard, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Safety Zone; Big Foot TLP, Walker Ridge 29, Outer Continental Shelf on the Gulf of Mexico'' ((RIN1625–AA00) (Docket No. USCG–2015–0863)) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2521. A communication from the Attorney-Advisor, U.S. Coast Guard, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Safety Zone; Red Bull GRC Air Show, Detroit River, Detroit, MI'' ((RIN1625–AA00) (Docket No. USCG–2015–0618)) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2522. A communication from the Attorney-Advisor, U.S. Coast Guard, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Safety Zone; Cleveland Triathlon, Lake Erie, North Coast Harbor, Cleveland, OH'' ((RIN1625–AA00) (Docket No. USCG–2015–0659)) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2523. A communication from the Attorney-Advisor, U.S. Coast Guard, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Safety Zone; Fall River Grand Prix, Mt. Hope Bay and Taunton River, Fall River, MA'' ((RIN1625–AA00) (Docket No. USCG–2015–0613)) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2524. A communication from the Attorney-Advisor, U.S. Coast Guard, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Safety Zone; Oswego Harborfest Jet Ski Show; Oswego Harbor, Oswego, NY'' ((RIN1625–AA00) (Docket No. USCG–2015–0507)) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2525. A communication from the Attorney-Advisor, U.S. Coast Guard, Department of Homeland Security, transmitting, pursuant to law, the report of a rule entitled ''Safety Zone; Maritime Museum Party, San Diego Bay; San Diego, CA'' ((RIN1625–AA00) (Docket No. USCG–2015–0647)) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2526. A communication from the Management and Program Analyst, Federal Aviation Administration, Department of Transportation, transmitting, pursuant to law, the report of a rule entitled ''Airworthiness Directives; GE Aviation Czech s.r.o. Turboprop Engines'' ((RIN2120–AA64) (Docket No. FAA–2015–0482)) received in the Office of the President of the Senate on August 3, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2527. A communication from the Acting Director, Office of Sustainable Fisheries, Department of Commerce, transmitting, pursuant to law, the report of a rule entitled ''Snapper-Grouper Fishery of the South Atlantic; 2015 Commercial Accountability Measure and Closure for Atlantic Dolphin'' (RIN0648–XE002) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2528. A communication from the Acting Director, Office of Sustainable Fisheries, Department of Commerce, transmitting, pursuant to law, the report of a rule entitled ''Fisheries of the Caribbean, Gulf of Mexico, and South Atlantic; 2015 Commercial Accountability Measure and Closure for South Atlantic Snowy Grouper'' (RIN0648–XE003) received in the Office of the President of the Senate on July 29, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2529. A communication from the Attorney-Advisor, Federal Highway Administration, Department of Transportation, transmitting, pursuant to law, the report of a rule entitled ''National Tunnel Inspection Standards'' (RIN2125–AF24) received in the Office of the President of the Senate on August 3, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2530. A communication from the Regulatory Ombudsman, Federal Motor Carrier Safety Administration, Department of Transportation, transmitting, pursuant to law, the report of a rule entitled ''State Compliance With Commercial Driver's License Program: Correction'' (RIN2126–AB80) received in the Office of the President of the Senate on August 3, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2531. A communication from the Chair of the Incentive Auctions Task Force, Office of Strategic Planning and Policy Analysis, Federal Communications Commission, transmitting, pursuant to law, the report of a rule entitled ''Expanding the Economic and Innovation Opportunities of Spectrum Through Incentive Auctions'' (FCC 15–69) received in the Office of the President of the Senate on

August 3, 2015; to the Committee on Commerce, Science, and Transportation.

EC–2532. A communication from the Chief of Staff, Media Bureau, Federal Communications Commission, transmitting, pursuant to law, the report of a rule entitled ''Expanding the Economic and Innovation Opportunities of Spectrum Through Incentive Auctions; Channel Sharing by Full Power and Class A Stations Outside the Broadcast Television Spectrum Incentive Auction Context'' ((GN Docket No. 12–268) (MB Docket No. 15–137) (FCC 15–67)) received in the Office of the President of the Senate on August 3, 2015; to the Committee on Commerce, Science, and Transportation.

PETITIONS AND MEMORIALS

The following petitions and memorials were laid before the Senate and were referred or ordered to lie on the table as indicated:

POM–74. A concurrent resolution adopted by the General Assembly of the State of Ohio urging the United States Congress to provide an adequate budget for the Department of Energy and the Nuclear Regulatory Commission to establish rules relative to environmentally friendly energy; to the Committee on Energy and Natural Resources.

AMENDED HOUSE CONCURRENT RESOLUTION NUMBER 9

Whereas, Ohio has many finite natural energy resources; and

Whereas, World energy demand and usage are expected to increase; and

Whereas, It is vital to the country's energy future to provide abundant base-load power and peaking energy-on-demand power affordably; and

Whereas, Extending Ohio's current energy boom will rest in creating a long-term energy plan and developing clean and affordable energy technologies such as liquid core molten salt reactors and small modular reactors; and

Whereas, America possesses a nearly inexhaustible supply of thorium and uranium (more than a billion years) that dramatically exceeds all known potential energy reserves; and

Whereas, The elements thorium and uranium have the practical potential to provide unlimited energy resources for Ohioans and Americans on demand in the near future and to provide many other tangible benefits; and

Whereas, Better utilization of thorium and uranium in specially designed reactors such as molten salt reactors, including liquid fluoride thorium reactors, can provide energy security from other nations by utilizing Ohio coal and a reactor's nuclear heat energy to produce an abundance of synthetic liquid transportation fuels. These synthetic fuels can be produced for many future generations of Ohioans in a safe, affordable, and in a most environmentally friendly manner; and

Whereas, The efficient use of thorium or uranium in a specially designed molten salt reactor allows for greatly increased environmentally friendly energy production that improves the economics of many recycling technologies and raises the standard of living; and

Whereas, It is incumbent upon Ohio legislators to be forward-thinking in addressing the future energy challenges for the next generation of Ohioans; and

Whereas, Ohio is uniquely capable to commercialize small modular reactors, liquid core molten salt reactors, and integral fast reactors with its research and development assets of the National Aeronautics and Space Administration Plum Brook (Sandusky, Ohio), the National Aeronautics and Space Administration John H. Glenn Research Center (Cleveland, Ohio area), the Wright-Patterson Air Force Base (Dayton, Ohio), USEC's uranium-enrichment facility (Piketon, Ohio), The Ohio State University's nuclear-research-and-development facilities (Columbus, Ohio), and other private companies and nonprofit organizations that specialize in nuclear-technology development in Ohio; and

Whereas, The academic, scientific, manufacturing, and business communities in Ohio have some of the best talent and research and development records in the world. Development of this groundbreaking and economic game-changing technology would serve Ohio's and America's economy better than current federal efforts to develop this technology in partnership with China; and

Whereas, Advanced technology using thorium and uranium can affordably provide medical isotopes of materials for medical uses such as treating cancer and HIV/AIDS, diagnostic procedures, and improved health care; and

Whereas, S.99, the ''American Medical Isotopes Production Act of 2011,'' was signed into law by President Barack Obama on January 2, 2013, and mandates a reliable domestic supply of molybdenum–99 for medical imaging and diagnostics; and

Whereas, Molybdenum-99 is used in more than sixteen million medical procedures annually in the United States; and

Whereas, No domestic supply of molybdenum–99 currently exists, and present suppliers use old reactors that result in frequent supply disruptions; and

Whereas, The Nuclear Regulatory Commission, charged with licensing nuclear reactors, is not well-funded for establishing procedures for new, advanced reactor designs based on different architectures from today's fleet of light water reactors; and

Whereas, Small modular reactors and liquid core molten salt reactors represent a business opportunity that Ohio's manufacturing base is well-suited to exploit. This could potentially result in creating forty thousand manufacturing jobs in total within Ohio, because these jobs have the ability to complement Ohio's coal industry, oil industry, and natural gas hydraulic fracturing industry by increasing jobs in those industries: Now, therefore, be it

Resolved, That we, the members of the 131st General Assembly of the State of Ohio, make the following recommendation for solutions to energy and medical-isotopes production; and be it further

Resolved, That the State of Ohio shall create a long-term energy plan that addresses the long-term energy needs of the country; and be it further

Resolved, That the State of Ohio shall encourage the research and development of liquid-core-molten-salt-reactors and small-modular-reactors technologies as a long-term solution to Ohio's energy needs; and be it further

Resolved, That the State of Ohio shall advocate that the Congress of the United States mandate, and provide an adequate budget for, the Department of Energy and the Nuclear Regulatory Commission to establish rules for manufacturing, siting, and licensing of small modular reactors and liquid core molten salt reactors to be built and operated in the United States by private industry for the production of energy and medical isotopes; and be it further

Resolved, That the State of Ohio shall invest in, seek to acquire grants for, implement programs for, encourage its institutions of higher learning to conduct research into, and attract companies for the development of future technologies that will provide greater energy resources more affordably, abundantly, and in a more environmentally friendly manner than is being done at present; and be it further

Resolved, That the Clerk of the House of Representatives transmit duly authenticated copies of this resolution to the President of the United States, the Secretary of the United States Department of Energy, the Commissioners of the Nuclear Regulatory Commission, the Speaker and Clerk of the United States House of Representatives, the President Pro Tempore and Secretary of the United States Senate, each member of the Ohio Congressional delegation, and the news media of Ohio.

POM–75. A petition by a citizen from the State of Texas urging the United States Congress to propose an amendment to the United States Constitution relative to establishing a procedure by which the President of the United States could be removed from office by means of a nationwide recall election; to the Committee on the Judiciary.

REPORTS OF COMMITTEES

The following reports of committees were submitted:

By Mr. THUNE, from the Committee on Commerce, Science, and Transportation, with an amendment in the nature of a substitute:

H.R. 719. A bill to require the Transportation Security Administration to conform to existing Federal law and regulations regarding criminal investigator positions, and for other purposes (Rept. No. 114–111).

By Mr. BLUNT, from the Committee on Rules and Administration:

Report to accompany S. Res. 73, An original resolution authorizing expenditures by committees of the Senate for the periods March 1, 2015 through September 30, 2015, October 1, 2015 through September 30, 2016, and October 1, 2016 through February 28, 2017 (Rept. No. 114–112).

By Mr. JOHNSON, from the Committee on Homeland Security and Governmental Affairs, with an amendment in the nature of a substitute and an amendment to the title:

S. 280. A bill to improve the efficiency, management, and interagency coordination of the Federal permitting process through reforms overseen by the Director of the Office of Management and Budget, and for other purposes (Rept. No. 114–113).

By Mr. BARRASSO, from the Committee on Indian Affairs, without amendment:

S. 986. A bill to require the Secretary of the Interior to take into trust 4 parcels of Federal land for the benefit of certain Indian Pueblos in the State of New Mexico (Rept. No. 114–114).

By Mr. THUNE, from the Committee on Commerce, Science, and Transportation, without amendment:

H.R. 1020. A bill to define STEM education to include computer science, and to support existing STEM education programs at the National Science Foundation (Rept. No. 114–115).

By Mr. JOHNSON, from the Committee on Homeland Security and Governmental Affairs, without amendment:

H.R. 1531. A bill to amend title 5, United States Code, to provide a pathway for temporary seasonal employees in Federal land management agencies to compete for vacant permanent positions under internal merit promotion procedures, and for other purposes.

EXECUTIVE REPORTS OF COMMITTEE

The following executive reports of nominations were submitted:

By Mr. McCAIN for the Committee on Armed Services.

*Joyce Louise Connery, of Massachusetts, to be a Member of the Defense Nuclear Facilities Safety Board for a term expiring October 18, 2019.

*Joseph Bruce Hamilton, of Texas, to be a Member of the Defense Nuclear Facilities Safety Board for the remainder of the term expiring October 18, 2016.

Army nomination of Brig. Gen. David S. Baldwin, to be Major General.

Air Force nomination of Col. Aaron M. Prupas, to be Brigadier General.

Army nomination of Gen. Mark A. Milley, to be General.

Navy nomination of Adm. John M. Richardson, to be Admiral.

Air Force nomination of Col. Christopher P. Azzano, to be Brigadier General.

Marine Corps nomination of Lt. Gen. Robert B. Neller, to be General.

Air Force nomination of Brig. Gen. Theron G. Davis, to be Major General.

Army nomination of Maj. Gen. John M. Murray, to be Lieutenant General.

Army nomination of Lt. Gen. Anthony R. Ierardi, to be Lieutenant General.

Army nomination of Brig. Gen. Garrett S. Yee, to be Major General.

Army nomination of Brig. Gen. Patrick J. Reinert, to be Major General.

Navy nomination of Vice Adm. James F. Caldwell, Jr., to be Admiral.

Navy nomination of Vice Adm. Joseph P. Aucoin, to be Vice Admiral.

Navy nomination of Capt. Cedric E. Pringle, to be Rear Admiral (lower half).

Army nominations beginning with Colonel Brett W. Andersen and ending with Colonel David E. Wood, which nominations were received by the Senate and appeared in the Congressional Record on July 23, 2015.

Army nomination of Col. Laura L. Yeager, to be Brigadier General.

Army nomination of Col. William J. Edwards, to be Brigadier General.

Army nomination of Brig. Gen. Robert W. Enzenauer, to be Major General.

Army nominations beginning with Brigadier General Randy A. Alewel and ending with Brigadier General Joanne F. Sheridan, which nominations were received by the Senate and appeared in the Congressional Record on July 23, 2015.

Marine Corps nomination of Maj. Gen. Rex C. McMillian, to be Lieutenant General.

Marine Corps nomination of Lt. Gen. Robert R. Ruark, to be Lieutenant General.

Air Force nomination of Lt. Gen. Samuel D. Cox, to be Lieutenant General.

Air Force nomination of Maj. Gen. Gina M. Grosso, to be Lieutenant General.

Navy nomination of Vice Adm. Paul A. Grosklags, to be Vice Admiral.

Mr. McCAIN. Mr. President, for the Committee on Armed Services I report favorably the following nomination lists which were printed in the RECORDs on the dates indicated, and ask unanimous consent, to save the expense of reprinting on the Executive Calendar that these nominations lie at the Secretary's desk for the information of Senators.

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

Air Force nomination of Jesse L. Johnson, to be Major.

Air Force nomination of Jose M. Goyos, to be Major.

Air Force nomination of John C. Boston, to be Colonel.

Air Force nomination of John A. Christ, to be Colonel.

Air Force nomination of Richard H. Fillman, Jr., to be Colonel.

Army nomination of Thomas M. Cherepko, to be Major.

Army nomination of Eric R. Davis, to be Lieutenant Colonel.

Army nomination of Stephen T. Wolpert, to be Colonel.

Army nomination of Jenifer E. Hey, to be Lieutenant Colonel.

Army nomination of Michael R. Starkey, to be Major.

Army nomination of Deepa Hariprasad, to be Major.

Army nomination of Dale T. Waltman, to be Colonel.

Army nominations beginning with Vincent E. Buggs and ending with James M. Zepp III, which nominations were received by the Senate and appeared in the Congressional Record on July 23, 2015.

Army nominations beginning with Shontelle C. Adams and ending with Joseph S. Zuffanti, which nominations were received by the Senate and appeared in the Congressional Record on July 23, 2015.

Army nominations beginning with Andrea C. Alicea and ending with Giovanny F. Zalamar, which nominations were received by the Senate and appeared in the Congressional Record on July 23, 2015.

Army nominations beginning with Eric B. Abdul and ending with Sara I. Zoesch, which nominations were received by the Senate and appeared in the Congressional Record on July 23, 2015.

Army nominations beginning with Gary S. Anselmo and ending with John G. Zierdt, which nominations were received by the Senate and appeared in the Congressional Record on July 23, 2015.

Army nominations beginning with Dean R. Klenz and ending with James J. Riche, which nominations were received by the Senate and appeared in the Congressional Record on July 29, 2015.

Army nominations beginning with Richard L. Bailey and ending with Kenneth S. Shedarowich, which nominations were received by the Senate and appeared in the Congressional Record on July 29, 2015.

Army nominations beginning with William Andino and ending with Christopher P. Willard, which nominations were received by the Senate and appeared in the Congressional Record on July 29, 2015.

Army nominations beginning with David B. Anderson and ending with Carl W. Thurmond, which nominations were received by the Senate and appeared in the Congressional Record on July 29, 2015.

Army nominations beginning with Jerry G. Baumgartner and ending with Mauri M. Thomas, which nominations were received by the Senate and appeared in the Congressional Record on July 29, 2015.

Army nominations beginning with Elizabeth A. Anderson and ending with Margaret L. Young, which nominations were received by the Senate and appeared in the Congressional Record on July 29, 2015.

Army nominations beginning with Tonia M. Crowley and ending with Cheryl M. K. Zeise, which nominations were received by the Senate and appeared in the Congressional Record on July 29, 2015.

Army nominations beginning with Jennifer M. Ahrens and ending with Todd W. Traver, which nominations were received by the Senate and appeared in the Congressional Record on July 29, 2015.

Army nominations beginning with Ramie K. Barfuss and ending with Dentonio Worrell, which nominations were received by the Senate and appeared in the Congressional Record on July 29, 2015.

Army nominations beginning with David J. Adam and ending with Victor Y. Yu, which nominations were received by the Senate and appeared in the Congressional Record on July 29, 2015.

Army nominations beginning with April Critelli and ending with Gregg A. Vigeant, which nominations were received by the Senate and appeared in the Congressional Record on July 29, 2015.

Army nominations beginning with Thomas F. Caldwell and ending with Bronson B. White, which nominations were received by the Senate and appeared in the Congressional Record on July 29, 2015.

Army nominations beginning with Carol L. Coppock and ending with Marie N. Wright, which nominations were received by the Senate and appeared in the Congressional Record on July 29, 2015.

Army nominations beginning with Norman S. Chun and ending with Harry W. Hatch, which nominations were received by the Senate and appeared in the Congressional Record on July 29, 2015.

Army nominations beginning with Lavetta L. Bennett and ending with Craig W. Strong, which nominations were received by the Senate and appeared in the Congressional Record on July 29, 2015.

Navy nomination of Audry T. Oxley, to be Lieutenant Commander.

Navy nomination of Mark B. Lyles, to be Captain.

Navy nominations beginning with Russell P. Bates and ending with Horacio G. Tan, which nominations were received by the Senate and appeared in the Congressional Record on July 23, 2015.

Navy nominations beginning with Sylvester C. Adamah and ending with Chadwick D. White, which nominations were received by the Senate and appeared in the Congressional Record on July 23, 2015.

Navy nominations beginning with Ruben A. Alcocer and ending with Melissia A. Williams, which nominations were received by the Senate and appeared in the Congressional Record on July 23, 2015.

Navy nominations beginning with Accursia A. Baldassano and ending with Jacqueline R. Williams, which nominations were received by the Senate and appeared in the Congressional Record on July 23, 2015.

Navy nominations beginning with Jason S. Ayeroff and ending with Brent E. Troyan, which nominations were received by the Senate and appeared in the Congressional Record on July 23, 2015.

Navy nominations beginning with Jerry J. Bailey and ending with Erin R. Wilfong, which nominations were received by the Senate and appeared in the Congressional Record on July 23, 2015.

Navy nominations beginning with William M. Anderson and ending with Jeffrey R. Wessel, which nominations were received by the Senate and appeared in the Congressional Record on July 23, 2015.

Navy nominations beginning with Maria A. Alavanja and ending with Vincent A. I. Zizak, which nominations were received by the Senate and appeared in the Congressional Record on July 23, 2015.

*Nomination was reported with recommendation that it be confirmed subject to the nominee's commitment to respond to requests to appear and testify before any duly constituted committee of the Senate.

(Nominations without an asterisk were reported with the recommendation that they be confirmed.)

INTRODUCTION OF BILLS AND JOINT RESOLUTIONS

The following bills and joint resolutions were introduced, read the first and second times by unanimous consent, and referred as indicated:

By Mr. LANKFORD (for himself, Mr. PORTMAN, Mr. MCCAIN, Mr. INHOFE, Mr. CASSIDY, Mr. CRUZ, Mr. BLUNT, Mr. BOOZMAN, Mr. CORKER, Mr. COATS, Mr. DAINES, Mr. SASSE, Mr. ISAKSON, and Mr. MORAN):

S. 1919. A bill to amend the Patient Protection and Affordable Care Act to protect rights of conscience with regard to requirements for coverage of specific items and services, to amend the Public Health Service Act to prohibit certain abortion-related discrimination in governmental activities, and for other purposes; to the Committee on Health, Education, Labor, and Pensions.

By Mr. DONNELLY (for himself and Mr. HELLER):

S. 1920. A bill to require the Comptroller General of the United States to develop and submit to Congress a biennial report on the current state of the skills gap in the United States, as of the date of the report, that includes an analysis of the effectiveness of efforts to close the skills gap and policy recommendations to improve such efforts, and for other purposes; to the Committee on Health, Education, Labor, and Pensions.

By Mr. MURPHY:

S. 1921. A bill to amend title XIX of the Social Security Act to encourage States to adopt administrative procedures with respect to nonmedical exemptions for State immunization requirements; to the Committee on Finance.

By Mr. HATCH (for himself, Mr. COATS, Mr. LANKFORD, and Mr. BLUNT):

S. 1922. A bill to amend titles II and XVI of the Social Security Act to provide for quality reviews of benefit decisions, and for other purposes; to the Committee on Finance.

By Mr. HATCH (for himself, Mr. COATS, Mr. LANKFORD, and Mr. BLUNT):

S. 1923. A bill to amend titles II and XVI of the Social Security Act to provide certain individuals with information on employment support services; to the Committee on Finance.

By Mr. THUNE (for himself and Mr. ROUNDS):

S. 1924. A bill to transfer administrative jurisdiction over certain Bureau of Land Management land from the Secretary of the Interior to the Secretary of Veterans Affairs for inclusion in the Black Hills National Cemetery, and for other purposes; to the Committee on Energy and Natural Resources.

By Mr. HEINRICH (for himself, Mr. WYDEN, Mr. UDALL, Mr. BENNET, Mr. MARKEY, Mr. SCHATZ, Mr. MERKLEY, Mr. COONS, Mr. PETERS, Mr. TESTER, Ms. BALDWIN, Mr. KING, Mr. LEAHY, and Mrs. SHAHEEN):

S. 1925. A bill to extend the secure rural schools and community self-determination program and to make permanent the payment in lieu of taxes program and the land and water conservation fund; to the Committee on Energy and Natural Resources.

By Ms. MIKULSKI (for herself and Ms. AYOTTE):

S. 1926. A bill to ensure access to screening mammography services; to the Committee on Finance.

By Mr. COATS (for himself and Mr. LANKFORD):

S. 1927. A bill to amend title 5, United States Code, to postpone the effective date of high-impact rules pending judicial review; to the Committee on Homeland Security and Governmental Affairs.

By Mr. TESTER (for himself, Mr. FRANKEN, and Mr. HEINRICH):

S. 1928. A bill to support the education of Indian children; to the Committee on Indian Affairs.

By Mr. HATCH (for himself, Mr. COATS, Mr. LANKFORD, and Mr. BLUNT):

S. 1929. A bill to amend the Social Security Act to prevent disability fraud, and for other purposes; to the Committee on Finance.

By Mr. ISAKSON (for himself and Mr. PERDUE):

S. 1930. A bill to adjust the boundary of the Kennesaw Mountain National Battlefield Park to include the Wallis House and Harriston Hill, and for other purposes; to the Committee on Energy and Natural Resources.

By Mr. MORAN (for himself and Mr. TESTER):

S. 1931. A bill to reaffirm that certain land has been taken into trust for the benefit of certain Indian tribes; to the Committee on Indian Affairs.

By Mr. BENNET:

S. 1932. A bill to provide States with flexibility to use Federal IV–E funding for State child welfare programs to improve safety, permanency, and well-being outcomes for all children who need child welfare services; to the Committee on Finance.

By Mr. CORKER (for himself, Mr. CARDIN, Mr. GRAHAM, Mr. DURBIN, Mr. ISAKSON, Mr. MARKEY, Ms. COLLINS, Mr. MENENDEZ, Mr. GARDNER, Mrs. SHAHEEN, Mr. KIRK, Mr. COONS, Mr. ALEXANDER, Mr. MURPHY, Mr. BOOZMAN, Mrs. MURRAY, and Mr. SCHUMER):

S. 1933. A bill to establish a comprehensive United States Government policy to encourage the efforts of countries in sub-Saharan Africa to develop an appropriate mix of power solutions, including renewable energy, for more broadly distributed electricity access in order to support poverty reduction, promote development outcomes, and drive economic growth, and for other purposes; to the Committee on Foreign Relations.

By Mr. BOOKER (for himself, Mrs. GILLIBRAND, Mrs. MURRAY, Mr. COONS, and Mr. PETERS):

S. 1934. A bill to amend the Small Business Investment Act of 1958 to establish the Scale-up Manufacturing Investment Company (''SUMIC'') Program; to the Committee on Small Business and Entrepreneurship.

By Ms. BALDWIN (for herself, Mr. KING, Mr. WYDEN, and Mr. PETERS):

S. 1935. A bill to require the Secretary of Commerce to undertake certain activities to support waterfront community revitalization and resiliency; to the Committee on Commerce, Science, and Transportation.

By Mr. UDALL (for himself and Mr. HEINRICH):

S. 1936. A bill to provide for drought preparedness measures in the State of New Mexico, and for other purposes; to the Committee on Energy and Natural Resources.

By Mr. UDALL:

S. 1937. A bill to amend the Richard B. Russell National School Lunch Act and the Child Nutrition Act of 1966 to improve nutrition in tribal areas, and for other purposes; to the Committee on Agriculture, Nutrition, and Forestry.

ADDITIONAL COSPONSORS

S. 258

At the request of Mr. ROBERTS, the name of the Senator from Arkansas (Mr. BOOZMAN) was added as a cosponsor of S. 258, a bill to amend title XVIII of the Social Security Act to remove the 96-hour physician certification requirement for inpatient critical access hospital services.

S. 314

At the request of Mr. GRASSLEY, the name of the Senator from Wyoming (Mr. BARRASSO) was added as a cosponsor of S. 314, a bill to amend title XVIII of the Social Security Act to provide for coverage under the Medicare program of pharmacist services.

S. 356

At the request of Mr. LEE, the names of the Senator from New Mexico (Mr. UDALL), the Senator from Hawaii (Mr. SCHATZ) and the Senator from Nevada (Mr. HELLER) were added as cosponsors of S. 356, a bill to improve the provisions relating to the privacy of electronic communications.

S. 779

At the request of Mr. CORNYN, the name of the Senator from Wisconsin (Mr. JOHNSON) was added as a cosponsor of S. 779, a bill to provide for Federal agencies to develop public access policies relating to research conducted by employees of that agency or from funds administered by that agency.

S. 849

At the request of Mr. ISAKSON, the name of the Senator from Delaware (Mr. CARPER) was added as a cosponsor of S. 849, a bill to amend the Public Health Service Act to provide for systematic data collection and analysis and epidemiological research regarding Multiple Sclerosis (MS), Parkinson's disease, and other neurological diseases.

S. 1049

At the request of Ms. HEITKAMP, the name of the Senator from Illinois (Mr. DURBIN) was added as a cosponsor of S. 1049, a bill to allow the financing by United States persons of sales of agricultural commodities to Cuba.

S. 1065

At the request of Mrs. GILLIBRAND, the name of the Senator from New York (Mr. SCHUMER) was added as a cosponsor of S. 1065, a bill to amend title IV of the Elementary and Secondary Education Act of 1965 to provide grants for the development of asthma management plans and the purchase of asthma inhalers and spacers for emergency use, as necessary.

S. 1085

At the request of Mrs. MURRAY, the names of the Senator from Virginia (Mr. WARNER) and the Senator from Michigan (Mr. PETERS) were added as cosponsors of S. 1085, a bill to expand eligibility for the program of comprehensive assistance for family caregivers of the Department of Veterans Affairs, to expand benefits available to participants under such program, to enhance special compensation for members of the uniformed services who require assistance in everyday life, and for other purposes.

S. 1121

At the request of Ms. AYOTTE, the name of the Senator from Florida (Mr. NELSON) was added as a cosponsor of S. 1121, a bill to amend the Horse Protection Act to designate additional unlawful acts under the Act, strengthen penalties for violations of the Act, improve Department of Agriculture enforcement of the Act, and for other purposes.

S. 1314

At the request of Mr. BOOKER, the name of the Senator from Oregon (Mr. WYDEN) was added as a cosponsor of S. 1314, a bill to establish an interim rule for the operation of small unmanned aircraft for commercial purposes and their safe integration into the national airspace system.

S. 1360

At the request of Mr. NELSON, the name of the Senator from Pennsylvania (Mr. CASEY) was added as a cosponsor of S. 1360, a bill to amend the limitation on liability for passenger rail accidents or incidents under section 28103 of title 49, United States Code, and for other purposes.

S. 1382

At the request of Mrs. GILLIBRAND, the names of the Senator from Maryland (Mr. CARDIN) and the Senator from California (Mrs. FEINSTEIN) were added as cosponsors of S. 1382, a bill to prohibit discrimination in adoption or foster care placements based on the sexual orientation, gender identity, or marital status of any prospective adoptive or foster parent, or the sexual orientation or gender identity of the child involved.

S. 1466

At the request of Mr. KIRK, the name of the Senator from Nevada (Mr. HELLER) was added as a cosponsor of S. 1466, a bill to amend title XVIII of the Social Security Act to modify payment under the Medicare program for outpatient department procedures that utilize drugs as supplies, and for other purposes.

S. 1491

At the request of Mr. BROWN, the name of the Senator from Wisconsin (Ms. BALDWIN) was added as a cosponsor of S. 1491, a bill to provide sensible relief to community financial institutions, to protect consumers, and for other purposes.

S. 1532

At the request of Mrs. MURRAY, the name of the Senator from Rhode Island (Mr. REED) was added as a cosponsor of S. 1532, a bill to ensure timely access to affordable birth control for women.

S. 1617

At the request of Mr. ISAKSON, his name was added as a cosponsor of S. 1617, a bill to prevent Hizballah and associated entities from gaining access to international financial and other institutions, and for other purposes.

S. 1632

At the request of Ms. COLLINS, the name of the Senator from Hawaii (Ms. HIRONO) was added as a cosponsor of S. 1632, a bill to require a regional strategy to address the threat posed by Boko Haram.

S. 1659

At the request of Mr. LEAHY, the names of the Senator from North Dakota (Ms. HEITKAMP), the Senator from Hawaii (Ms. HIRONO) and the Senator from Rhode Island (Mr. REED) were added as cosponsors of S. 1659, a bill to amend the Voting Rights Act of 1965 to revise the criteria for determining which States and political subdivisions are subject to section 4 of the Act, and for other purposes.

S. 1709

At the request of Ms. WARREN, the name of the Senator from Wisconsin (Ms. BALDWIN) was added as a cosponsor of S. 1709, a bill to reduce risks to the financial system by limiting banks' ability to engage in certain risky activities and limiting conflicts of interest, to reinstate certain Glass-Steagall Act protections that were repealed by the Gramm-Leach-Bliley Act, and for other purposes.

S. 1819

At the request of Mr. DAINES, the name of the Senator from Alabama (Mr. SESSIONS) was added as a cosponsor of S. 1819, a bill to improve security at Armed Forces recruitment centers.

S. 1844

At the request of Mr. HOEVEN, the name of the Senator from Florida (Mr. NELSON) was added as a cosponsor of S. 1844, a bill to amend the Agricultural Marketing Act of 1946 to provide for voluntary country of origin labeling for beef, pork, and chicken.

S. 1897

At the request of Mr. SCOTT, the name of the Senator from New York (Mrs. GILLIBRAND) was added as a cosponsor of S. 1897, a bill to help keep law enforcement officers and communities safer by making grants to purchase body worn cameras for use by State, local, and tribal law enforcement officers.

S. 1911

At the request of Ms. COLLINS, the name of the Senator from Illinois (Mr. KIRK) was added as a cosponsor of S. 1911, a bill to implement policies to end preventable maternal, newborn, and child deaths globally.

S. 1912

At the request of Mr. TESTER, the name of the Senator from Hawaii (Ms. HIRONO) was added as a cosponsor of S. 1912, a bill to protect the rights of Indian and Native Alaskan voters.

S. 1918

At the request of Mr. MENENDEZ, the name of the Senator from Michigan (Mr. PETERS) was added as a cosponsor of S. 1918, a bill to amend the Endangered Species Act of 1973 to extend the import- and export-related provision of that Act to species proposed for listing as threatened or endangered under that Act.

S. RES. 148

At the request of Mr. KIRK, the name of the Senator from Maine (Ms. COLLINS) was added as a cosponsor of S. Res. 148, a resolution condemning the Government of Iran's state-sponsored persecution of its Baha'i minority and its continued violation of the International Covenants on Human Rights.

S. RES. 228

At the request of Ms. AYOTTE, the name of the Senator from Connecticut (Mr. BLUMENTHAL) was added as a cosponsor of S. Res. 228, a resolution designating September 2015 as ''National Ovarian Cancer Awareness Month''.

AMENDMENT NO. 2547

At the request of Mr. HELLER, the name of the Senator from Vermont (Mr. LEAHY) was added as a cosponsor of amendment No. 2547 intended to be proposed to S. 754, an original bill to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

AMENDMENT NO. 2548

At the request of Mr. HELLER, the name of the Senator from Vermont (Mr. LEAHY) was added as a cosponsor of amendment No. 2548 intended to be proposed to S. 754, an original bill to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. HATCH (for himself, Mr. COATS, Mr. LANKFORD, and Mr. BLUNT):

S. 1922. A bill to amend titles II and XVI of the Social Security Act to provide for quality reviews of benefit decisions, and for other purposes; to the Committee on Finance.

Mr. HATCH. Mr. President, I rise to speak once again on the Social Security Disability Insurance—or DI—Program. As everyone in this Chamber should know, the DI trust fund is projected to be exhausted next year. That means, absent any change in law, we will be seeing across-the-board benefit cuts of close to 20 percent for DI beneficiaries. Over the last several months, I have come to the floor on a handful of occasions to talk about this program and the imminent depreciation of its trust fund.

I have called on my colleagues on both sides of the aisle to work with me to address these issues. I will repeat that call today.

In addition, today I have introduced three separate bills that are designed to help update and improve the administration of the DI program. As we talk about solutions to address the depletion of the DI trust fund, we should also be talking about ways to update the DI program, ways to make it easier for beneficiaries who can and who desire to return to work to be able to explore those opportunities and ways to improve efforts to deter and prevent waste and fraud.

The first bill I introduced today would update and expand the Social Security Administration's tools to deter and punish fraudsters who cheat the system. The second bill would authorize the Commissioner of SSA to provide denied DI applicants with information about employment support services that are provided by both public agencies and private nonprofit organizations.

That information will help denied applicants find opportunities to reenter the workforce, instead of continually cycling through the DI application process. The third bill would require SSA to review hearing decisions by administrative law judges to ensure that they are following the law as well as Social Security regulations and policy. All three of these bills are designed to improve the administration of this disability program and make it work better for beneficiaries and taxpayers. They will not, by themselves, solve all of the program's fiscal problems, but they will improve the DI system.

More work will need to go into this effort, and as chairman of the committee with jurisdiction over the DI program, I am committed to solving these problems and preventing the massive benefit cuts we will see under current law. I would like to point out three things about my stated approach to dealing with the DI program.

First, you will note I have not used the word ''crisis'' to describe what is happening with the DI trust fund. Second, you would be hard-pressed to find any proposal I have submitted that could credibly be characterized as ''slashing'' DI benefits. Third, nothing I have put forward either today or in the past could conceivably be thought of as ''privatizing'' disability insurance.

I have to point this out because a number of people, including some of my friends on the other side of the aisle, have described the Republican efforts to address the DI trust fund depletion using some of those very same words.

These individuals are currently more interested in turning this issue and the coming benefit cuts into a political football than in actually solving the problem. My question is, What good will that do for the DI program or its beneficiaries? It is not just the DI program that has problems. Social Security, in general, faces a number of significant fiscal and policy challenges.

In their most recent report, the Social Security board of trustees, which includes several members of President Obama's Cabinet, recommended ''that lawmakers address the projected trust fund shortfalls in a timely way in order to phase in necessary changes gradually and give workers and beneficiaries time to adjust to them.''

That says to me the sooner we act to put Social Security on a sustainable fiscal path the better it is for Americans and their security. It clearly does not mean we should ignore the financial problems facing Social Security or kick the can down the road, hoping some future Congress will get its act together and solve the problems.

Of course, providing financial sustainability to Social Security is easier said than done. There are reasonable disagreements over how best to address Social Security's fiscal shortfalls, including different views on payroll tax revenues that fund the program and how quickly promised benefits will grow in the future. Yet we should not limit the discussion to taxes and outlays.

We also should look at how the program can be improved and brought up-to-date. For example, the vocational grids and medical guidelines that SSA uses in the disability program are woefully out of date, and much of the existing structure of Social Security's retirement program was developed long ago, when labor markets and work patterns were much different than they are today.

We should be working to address all of these challenges, both the fiscal and policy challenges now, instead of putting them off for later days. With respect to the DI program in particular, I have been working for some time now to obtain input from experts and stakeholders across the spectrum to figure out how we can make the program work better. Joined by House Ways and Means Committee Chairman RYAN and Social Security Subcommittee Chairman JOHNSON, I have solicited input from stakeholders in various venues and continue to welcome ideas or proposals from anyone who wants to submit them.

The bills I have dropped today are just the latest in a series of bills I have introduced to help jump-start the discussion of DI reforms. We should not sit idly by and wait for another financing cliff to appear around the end of next year. As the Social Security trustees made clear, the sooner Congress acts to address these shortcomings, the better. Neither DI beneficiaries nor taxpayers benefit from lingering uncertainty about how the impending trust fund depletion will be resolved.

As I have said many times, I am ready and willing to have this conversation. Sadly, up to now, I have heard nothing in response from the Obama administration and very little from my colleagues on the other side of the aisle. Anyone familiar with the current state of the DI trust fund would likely acknowledge that we are going to have to reallocate resources into the fund if we are going to prevent the impending benefit cuts from happening next year.

Most proposals I have seen, including those from the President's budget, involve a shuffling of money from Social Security's retirement fund to the DI trust fund, but even if we have to reallocate resources to shore up the DI program, we should not delay confronting the obvious need for reform. On this point, I will once again quote the most recent report from the Social Security trustees, which says, ''Reallocation of resources in the absence of substantive relief might serve to delay DI reforms and much-needed corrections for Social Security as a whole.''

It is true that as many of my colleagues have noted, there have been bipartisan agreements to reallocate resources within Social Security in the past. However, in virtually every case, the reallocations were accompanied by substantive policy changes. This time should be no different. The last time we reallocated resources from the retirement to the DI trust fund, DI awards were increasing unexpectedly and Congress needed to examine the reasons for this increase before acting to change the way the DI system worked.

At the time, most people agreed that reforms were necessary and that the reallocation would buy the time Congress needed to come up with those reforms, get them enacted, and put the trust fund on sound fiscal footing. That was more than 20 years ago. Sadly, though not surprisingly, Congress did not follow through with the reforms, and we now face another reserve depletion in the trust fund.

Needless to say, doubling down on the same strategy, a strategy that has already failed to produce the needed policy changes, is not a prudent course of action. In my view, any resource reallocation that gets enacted must be accompanied by changes in the DI program. However, the President does not seem to share this view. The administration has called for a stand-alone reallocation of payroll tax receipts away from the retirement and survivor's trust fund and into the DI trust fund.

This proposal would, depending on the estimate, extend the life of the DI program to the early 2030s, at which point both Social Security trust funds, disability and retirement, will be exhausted at the same time, triggering massive benefit cuts for all beneficiaries. In fact, there are those who would argue that the Social Security retirement fund is already exhausted and deeply in debt.

That is their idea of a responsible approach to a widely acknowledged fiscal problem. Outside of the stand-alone reallocation scheme, the President's budget offers precious little in the way of reforms to the DI program or Social Security in general. In other words, the Obama administration's entire answer to all of Social Security's many fiscal problems is literally to just let future Congress's and administrations deal with those problems.

This, to me, would be the height of irresponsibility. While it may not be possible, absent some kind of resource allocation, to keep the DI program's current promises between now and the end of the year, we can and should take meaningful steps now to improve the program. That is my goal. I hope enough of my colleagues share this goal to make it a reality.

If we are going to get there, it is going to require bipartisan cooperation on both ends of Pennsylvania Avenue. In other words, we are going to need to see more from the administration than we have seen thus far. It is already August. Despite my repeated requests to the administration and my friends on the other side of the aisle to engage

with me to work on this issue, I have yet to hear a meaningful response. I hope that will change.

There is no harm in discussing options. I am willing to discuss any and all options to fix these problems. There is, on the other hand, a great deal of potential harm to DI beneficiaries if we continue to ignore the problem while waiting for a financial cliff to force people's hands. Once again, I urge my friends on both sides of the aisle to engage on this issue now, and do not wait until it is too late to take meaningful action.

AMENDMENTS SUBMITTED AND PROPOSED

SA 2549. Mr. PETERS submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table.

SA 2550. Mr. PETERS submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2551. Mr. PETERS submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2552. Mr. COONS submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2553. Mr. SCHATZ submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2554. Mr. SCHATZ submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2555. Ms. HEITKAMP submitted an amendment intended to be proposed by her to the bill S. 754, supra; which was ordered to lie on the table.

SA 2556. Mr. LEE (for himself, Mr. LEAHY, Mr. DURBIN, and Mr. HELLER) submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2557. Ms. MIKULSKI (for herself, Mr. CARDIN, and Mr. WARNER) submitted an amendment intended to be proposed by her to the bill S. 754, supra; which was ordered to lie on the table.

SA 2558. Mr. BENNET (for himself and Mr. PORTMAN) submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2559. Mr. MANCHIN submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2560. Mr. MANCHIN submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2561. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2562. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2563. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2564. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2565. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2566. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2567. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2568. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2569. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2570. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2571. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2572. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2573. Mr. FLAKE submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2574. Mr. HATCH submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2575. Ms. HIRONO submitted an amendment intended to be proposed by her to the bill S. 754, supra; which was ordered to lie on the table.

SA 2576. Mr. MARKEY submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2577. Mr. MARKEY submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2578. Mr. VITTER (for himself and Mr. TESTER) submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2579. Mr. VITTER submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2580. Mr. FLAKE submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2581. Mr. COTTON submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2582. Mr. FLAKE (for himself and Mr. FRANKEN) submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2583. Ms. BALDWIN submitted an amendment intended to be proposed by her to the bill S. 754, supra; which was ordered to lie on the table.

SA 2584. Mr. BLUMENTHAL submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2585. Mr. BLUMENTHAL submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2586. Mr. HEINRICH (for himself and Ms. HIRONO) submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2587. Mr. LEAHY submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2588. Mrs. BOXER submitted an amendment intended to be proposed by her to the bill S. 754, supra; which was ordered to lie on the table.

SA 2589. Mr. MURPHY (for himself and Mr. HATCH) submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2590. Mr. CARDIN (for himself, Ms. MIKULSKI, Mr. WARNER, Mr. KAINE, and Ms. BALDWIN) submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2591. Mr. SANDERS submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2592. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2593. Mr. DURBIN submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2594. Mr. DURBIN submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2595. Mr. DURBIN submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2596. Mr. DURBIN submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2597. Mrs. SHAHEEN submitted an amendment intended to be proposed by her to the bill S. 754, supra; which was ordered to lie on the table.

SA 2598. Mr. FRANKEN submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2599. Mr. FRANKEN submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2600. Mr. FRANKEN submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2601. Mr. FRANKEN submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2602. Mr. FRANKEN submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2603. Mr. KIRK (for himself and Mrs. GILLIBRAND) submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2604. Mr. COATS submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2605. Ms. WARREN submitted an amendment intended to be proposed by her to the bill S. 754, supra; which was ordered to lie on the table.

SA 2606. Ms. WARREN submitted an amendment intended to be proposed by her to the bill S. 754, supra; which was ordered to lie on the table.

SA 2607. Ms. WARREN submitted an amendment intended to be proposed by her to the bill S. 754, supra; which was ordered to lie on the table.

SA 2608. Ms. WARREN submitted an amendment intended to be proposed by her to the bill S. 754, supra; which was ordered to lie on the table.

SA 2609. Ms. WARREN submitted an amendment intended to be proposed by her to the bill S. 754, supra; which was ordered to lie on the table.

SA 2610. Ms. KLOBUCHAR submitted an amendment intended to be proposed by her to the bill S. 754, supra; which was ordered to lie on the table.

SA 2611. Ms. KLOBUCHAR submitted an amendment intended to be proposed by her to the bill S. 754, supra; which was ordered to lie on the table.

SA 2612. Mr. FRANKEN (for himself, Mr. LEAHY, and Mr. WYDEN) submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2613. Mr. CARPER submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2614. Mr. CARPER submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2615. Mr. CARPER submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

TEXT OF AMENDMENTS

SA 2549. Mr. PETERS submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ____. CERTIFICATION FOR CYBERSECURITY AND INFORMATION ASSURANCE EDUCATION PROGRAMS.

The Secretary of Homeland Security, in collaboration with the National Cybersecurity Center of Excellence at the National Institute of Standards and Technology, shall develop a certification for existing cybersecurity and information assurance education programs, which shall be provided to those programs that provide training in proper procedure and protocol for sharing cyber threat indicators and protecting sensitive personally identifiable information.

SA 2550. Mr. PETERS submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ____. CYBERSECURITY AWARENESS CAMPAIGN.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended by adding at the end the following:

"SEC. 230. CYBERSECURITY AWARENESS CAMPAIGN.

''(a) IN GENERAL.—The Under Secretary for Cybersecurity and Infrastructure Protection shall develop and implement an ongoing and comprehensive cybersecurity awareness campaign regarding cybersecurity risks and voluntary best practices for mitigating and responding to such risks.

''(b) REQUIREMENTS.—The campaign developed under subsection (a) shall, at a minimum, publish and disseminate, on an ongoing basis, the following:

''(1) Public service announcements targeted at improving awareness among State, local, and tribal governments, the private sector, academia, and stakeholders in specific audiences, including the elderly, students, small businesses, members of the Armed Forces, and veterans.

''(2) Vendor and technology-neutral voluntary best practices information.

''(c) CONSULTATION.—The Under Secretary for Cybersecurity and Infrastructure Protection shall consult with a wide range of stakeholders in government, industry, academia, and the non-profit community in carrying out this section.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 226 (relating to cybersecurity recruitment and retention) the following:

''Sec. 230. Cybersecurity Awareness Campaign.''.

SA 2551. Mr. PETERS submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 12, between lines 7 and 8, insert the following:

(F) ensure collaboration with State, local and tribal governments to enhance the effectiveness of sharing cyber threat indicators and ensure cooperation to prevent, protect, mitigate, respond to, and recover from cybersecurity incidents.

SA 2552. Mr. COONS submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

Beginning on page 21, strike line 23 and all that follows through page 31, line 5 and insert the following:

(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 shared with the Federal Government by any entity pursuant to section 4 that are received through the process described in subsection (c) of this section and that satisfy the requirements of the guidelines developed under subsection (b)—

(i) are shared in an automated manner 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;

(B) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 4 in a manner other than the 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 Act, 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 Act, 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 Act 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 Act, 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 Act.

(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 Act that would be unlikely to include personal information of or identifying a specific person not necessary to describe or identify a cyber security threat.

(ii) Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be necessary to describe or identify a cybersecurity threat.

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

(b) PRIVACY AND CIVIL LIBERTIES.—

(1) GUIDELINES OF ATTORNEY GENERAL.—Not later than 60 days after the date of the enactment of this Act, 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 Act.

(2) FINAL GUIDELINES.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, 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 Act.

(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 Act;

(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 Act; 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 Act; 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 Act, 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 Act 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) shall require the Department of Homeland Security to review all cyber threat indicators and defensive measures received and remove any personal information of or identifying a specific person not necessary to identify or describe the cybersecurity threat before sharing such indicator or defensive measure with appropriate Federal entities;

(D) ensures that all of the appropriate Federal entities receive in an automated manner such cyber threat indicators as quickly as operationally possible from the Department of Homeland Security;

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

(F) 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 Act; 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 as quickly as operationally practicable with receipt through the process within the Department of Homeland Security.

SA 2553. Mr. SCHATZ submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

Strike paragraph (2) of section 3(b) and insert the following:

(2) COORDINATION AND CONSULTATION.—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, 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—

(A) consult with appropriate private entities; and

(B) coordinate with appropriate Federal entities, including the National Laboratories (as defined in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801)).

SA 2554. Mr. SCHATZ submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

Beginning on page 13, strike line 4, and all that follows through page 14, line 1.

SA 2555. Ms. HEITKAMP submitted an amendment intended to be proposed by her to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ____. ENHANCEMENT OF EMERGENCY SERVICES.

(a) COLLECTION OF DATA.—Not later than 90 days after the date of enactment of this Act, the Secretary of Homeland Security, acting through the National Cybersecurity and Communications Integration Center, in coordination with appropriate entities and the Director for Emergency Communications, shall establish a process by which a Statewide Interoperability Coordinator may report data on any cybersecurity risk or incident involving any information system or network used by emergency response providers (as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101)) within the State.

(b) ANALYSIS OF DATA.—Not later than 1 year after the date of enactment of this Act, the Secretary of Homeland Security, acting through the Director of the National Cybersecurity and Communications Integration Center, in coordination with appropriate entities and the Director for Emergency Communications, and in consultation with the Director of the National Institute of Standards and Technology, shall conduct integration and analysis of the data reported under subsection (a) to develop information and recommendations on security and resilience measures for any information system or network used by State emergency response providers.

(c) BEST PRACTICES.—

(1) IN GENERAL.—Using the results of the integration and analysis conducted under subsection (b), and any other relevant information, the Director of the National Institute of Standards and Technology shall, on an ongoing basis, facilitate and support the development of methods for reducing cybersecurity risks to emergency response providers using the process described in section 2(e) of the National Institute of Standards and Technology Act (15 U.S.C. 272(e)).

(2) REPORT.—The Director of the National Institute of Standards and Technology shall submit a report to Congress on the methods developed under paragraph (1) and shall make such report publically available on the website of the National Institute of Standards and Technology.

SA 2556. Mr. LEE (for himself, Mr. LEAHY, Mr. DURBIN, and Mr. HELLER) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE II—ELECTRONIC COMMUNICATIONS PRIVACY ACT AMENDMENTS

SEC. 201. SHORT TITLE.

This title may be cited as the ''Electronic Communications Privacy Act Amendments Act of 2015''.

SEC. 202. CONFIDENTIALITY OF ELECTRONIC COMMUNICATIONS.

Section 2702(a)(3) of title 18, United States Code, is amended to read as follows:

''(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge to any governmental entity the contents of any communication described in section 2703(a), or any record or other information pertaining to a subscriber or customer of such service.''.

SEC. 203. ELIMINATION OF 180-DAY RULE; SEARCH WARRANT REQUIREMENT; REQUIRED DISCLOSURE OF CUSTOMER RECORDS.

(a) IN GENERAL.—Section 2703 of title 18, United States Code, is amended—

(1) by striking subsections (a), (b), and (c) and inserting the following:

''(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS.—A governmental entity may require the disclosure by a provider of electronic communication service or remote computing service of the contents of a wire or electronic communication that is in electronic storage with or otherwise stored, held, or maintained by the provider only if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that is issued by a court of competent jurisdiction directing the disclosure.

''(b) NOTICE.—Except as provided in section 2705, not later than 10 business days in the case of a law enforcement agency, or not later than 3 business days in the case of any other governmental entity, after a governmental entity receives the contents of a wire or electronic communication of a subscriber or customer from a provider of electronic communication service or remote computing service under subsection (a), the governmental entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, as specified by the court issuing the warrant, the subscriber or customer—

''(1) a copy of the warrant; and

''(2) a notice that includes the information referred to in clauses (i) and (ii) of section 2705(a)(4)(B).

''(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—

''(1) IN GENERAL.—Subject to paragraph (2), a governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber or customer of the provider or service (not including the contents of communications), only if the governmental entity—

''(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that is issued by a court of competent jurisdiction directing the disclosure;

''(B) obtains a court order directing the disclosure under subsection (d);

''(C) has the consent of the subscriber or customer to the disclosure; or

''(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of the provider or service that is engaged in telemarketing (as defined in section 2325).

''(2) INFORMATION TO BE DISCLOSED.—A provider of electronic communication service or remote computing service shall, in response to an administrative subpoena authorized by Federal or State statute, a grand jury, trial, or civil discovery subpoena, or any means authorized under paragraph (1), disclose to a governmental entity the—

''(A) name;

''(B) address;

''(C) local and long distance telephone connection records, or records of session times and durations;

''(D) length of service (including start date) and types of service used;

''(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

''(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber or customer of such service.

''(3) NOTICE NOT REQUIRED.—A governmental entity that receives records or information under this subsection is not required to provide notice to a subscriber or customer.''; and

(2) by adding at the end the following:

''(h) RULE OF CONSTRUCTION.—Nothing in this section or in section 2702 shall be construed to limit the authority of a governmental entity to use an administrative subpoena authorized under a Federal or State statute or to use a Federal or State grand jury, trial, or civil discovery subpoena to—

''(1) require an originator, addressee, or intended recipient of an electronic communication to disclose the contents of the electronic communication to the governmental entity; or

''(2) require an entity that provides electronic communication services to the officers, directors, employees, or agents of the entity (for the purpose of carrying out their duties) to disclose the contents of an electronic communication to or from an officer, director, employee, or agent of the entity to a governmental entity, if the electronic communication is held, stored, or maintained on an electronic communications system owned or operated by the entity.''.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 2703(d) of title 18, United States Code, is amended—

(1) by striking ''A court order for disclosure under subsection (b) or (c)'' and inserting ''A court order for disclosure under subsection (c)''; and

(2) by striking ''the contents of a wire or electronic communication, or''.

SEC. 204. DELAYED NOTICE.

Section 2705 of title 18, United States Code, is amended to read as follows:

''§ 2705. Delayed notice

''(a) DELAY OF NOTIFICATION.—

''(1) IN GENERAL.—A governmental entity that is seeking a warrant under section 2703(a) may include in the application for the warrant a request for an order delaying the notification required under section 2703(b) for a period of not more than 180 days in the case of a law enforcement agency, or not more than 90 days in the case of any other governmental entity.

''(2) DETERMINATION.—A court shall grant a request for delayed notification made under paragraph (1) if the court determines that there is reason to believe that notification of the existence of the warrant may result in—

''(A) endangering the life or physical safety of an individual;

''(B) flight from prosecution;

''(C) destruction of or tampering with evidence;

''(D) intimidation of potential witnesses; or

''(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

''(3) EXTENSION.—Upon request by a governmental entity, a court may grant one or more extensions of the delay of notification granted under paragraph (2) of not more than 180 days in the case of a law enforcement agency, or not more than 90 days in the case of any other governmental entity.

''(4) EXPIRATION OF THE DELAY OF NOTIFICATION.—Upon expiration of the period of delay of notification under paragraph (2) or (3), the governmental entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective as specified by the court approving the search warrant, the customer or subscriber—

''(A) a copy of the warrant; and

''(B) notice that informs the customer or subscriber—

''(i) of the nature of the law enforcement inquiry with reasonable specificity;

''(ii) that information maintained for the customer or subscriber by the provider of electronic communication service or remote computing service named in the process or request was supplied to, or requested by, the governmental entity;

''(iii) of the date on which the warrant was served on the provider and the date on which the information was provided by the provider to the governmental entity;

''(iv) that notification of the customer or subscriber was delayed;

''(v) the identity of the court authorizing the delay; and

''(vi) of the provision of this chapter under which the delay was authorized.

''(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.—

''(1) IN GENERAL.—A governmental entity that is obtaining the contents of a communication or information or records under section 2703 may apply to a court for an order directing a provider of electronic communication service or remote computing service to which a warrant, order, subpoena, or other directive under section 2703 is directed not to notify any other person of the existence of the warrant, order, subpoena, or other directive for a period of not more than 180 days in the case of a law enforcement agency, or not more than 90 days in the case of any other governmental entity.

''(2) DETERMINATION.—A court shall grant a request for an order made under paragraph (1) if the court determines that there is reason to believe that notification of the existence of the warrant, order, subpoena, or other directive may result in—

''(A) endangering the life or physical safety of an individual;

''(B) flight from prosecution;

''(C) destruction of or tampering with evidence;

''(D) intimidation of potential witnesses; or

''(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

''(3) EXTENSION.—Upon request by a governmental entity, a court may grant one or more extensions of an order granted under paragraph (2) of not more than 180 days in the case of a law enforcement agency, or not more than 90 days in the case of any other governmental entity.

''(4) PRIOR NOTICE TO LAW ENFORCEMENT.—Upon expiration of the period of delay of notice under this section, and not later than 3 business days before providing notice to a customer or subscriber, a provider of electronic communication service or remote computing service shall notify the governmental entity that obtained the contents of a communication or information or records under section 2703 of the intent of the provider of electronic communication service or remote computing service to notify the customer or subscriber of the existence of the warrant, order, or subpoena seeking that information.

''(c) DEFINITION.—In this section and section 2703, the term 'law enforcement agency' means an agency of the United States, a State, or a political subdivision of a State, authorized by law or by a government agency to engage in or supervise the prevention, detection, investigation, or prosecution of any violation of criminal law, or any other Federal or State agency conducting a criminal investigation.''.

SEC. 205. EVALUATION BY THE GOVERNMENT ACCOUNTABILITY OFFICE.

Not later than September 30, 2017, the Comptroller General of the United States shall submit to Congress a report regarding the disclosure of customer communications and records under section 2703 of title 18, United States Code, which shall include—

(1) an analysis and evaluation of such disclosure under section 2703 of title 18, United States Code, as in effect before the date of enactment of this Act, including—

(A) a comprehensive analysis and evaluation regarding the number of individual instances, in each of the 5 years before the year in which this Act is enacted, in which Federal, State, or local law enforcement officers used section 2703 of title 18, United States Code, to obtain information relevant to an ongoing criminal investigation;

(B) an analysis of the average length of time taken by a provider of an electronic communication service or a remote computing service to comply with requests by law enforcement officers for information under section 2703 of title 18, United States Code;

(C) the number of individual instances, in each of the 5 years before the year in which this Act is enacted, in which information was requested by law enforcement officers from a provider of an electronic communication service or a remote computing service under a warrant as authorized under section 2703(a) of title 18, United States Code;

(D) the number of individual instances and type of request, in each of the 5 years before the year in which this Act is enacted, in which information was requested by law enforcement officers from a provider of an electronic communication service or a remote computing service under the other information request provisions in section 2703 of title 18, United States Code; and

(E) the number of individual instances, in each of the 5 years before the year in which this Act is enacted, in which law enforcement officers requested delayed notification to the subscriber or customer under section 2705 of title 18, United States Code; and

(2) an analysis and evaluation of such disclosure under section 2703 of title 18, United States Code, as amended by this title, including—

(A) an evaluation of the effects of the amendments to the warrant requirements on judges, court dockets, or any other court operations;

(B) a survey of Federal, State, and local judges and law enforcement officers to determine the average length of time required for providers of an electronic communication service or a remote computing service to provide the contents of communications requested under a search warrant, which shall include identifying the number of instances in which a judge was required to order a provider of an electronic communication service or a remote computing service to appear to show cause for failing to comply with a warrant or to issue an order of contempt against a provider of an electronic communication service or a remote computing service for such a failure; and

(C) determining whether the amendments to the warrant requirements resulted in an increase in the use of the emergency exception under section 2702(b)(8) of title 18, United States Code.

SEC. 206. RULE OF CONSTRUCTION.

Nothing in this title or an amendment made by this title shall be construed to preclude the acquisition by the United States Government of—

(1) the contents of a wire or electronic communication pursuant to other lawful authorities, including the authorities under chapter 119 of title 18 (commonly known as the ''Wiretap Act''), the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), or any other provision of Federal law not specifically amended by this title; or

(2) records or other information relating to a subscriber or customer of any electronic communications service or remote computing service (not including the content of such communications) pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), chapter 119 of title 18 (commonly known as the ''Wiretap Act''), or any other provision of Federal law not specifically amended by this title.

SA 2557. Ms. MIKULSKI (for herself, Mr. CARDIN, and Mr. WARNER) submitted an amendment intended to be proposed by her to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. FUNDING.

(a) IN GENERAL.—Effective on the date of enactment of this Act, there is appropriated, out of any money in the Treasury not otherwise appropriated, for the fiscal year ending September 30, 2015, an additional amount for the appropriations account appropriated under the heading ''SALARIES AND EXPENSES'' under the heading ''OFFICE OF PERSONNEL MANAGEMENT'', $37,000,000, to remain available until September 30, 2017, for accelerated cybersecurity in response to data breaches.

(b) EMERGENCY DESIGNATION.—The amount appropriated under subsection (a) is designated by the Congress as an emergency requirement pursuant to section 251(b)(2)(A)(i) of the Balanced Budget and Emergency Deficit Control Act of 1985, and shall be available only if the President subsequently so designates such amount and transmits such designation to the Congress.

SA 2558. Mr. BENNET (for himself and Mr. PORTMAN) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE II—FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT

SECTION 201. SHORT TITLE.

This title may be cited as the ''Federal Cybersecurity Workforce Assessment Act''.

SEC. 202. DEFINITIONS.

In this title:

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

(A) the Committee on Armed Services of the Senate;

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

(C) the Committee on Armed Services in the House of Representatives;

(D) the Committee on Homeland Security of the House of Representatives; and

(E) the Committee on Oversight and Government Reform of House of Representatives.

(2) DIRECTOR.—The term ''Director'' means the Director of the Office of Personnel Management.

(3) ROLES.—The term ''roles'' has the meaning given the term in the National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework.

SEC. 203. NATIONAL CYBERSECURITY WORKFORCE MEASUREMENT INITIATIVE.

(a) IN GENERAL.—The head of each Federal agency shall—

(1) identify all positions within the agency that require the performance of information technology, cybersecurity, or other cyber-related functions; and

(2) assign the corresponding employment code, which shall be added to the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework, in accordance with subsection (b).

(b) EMPLOYMENT CODES.—

(1) PROCEDURES.—

(A) CODING STRUCTURE.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Commerce, acting through the National Institute of Standards and Technology, shall update the National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework to include a corresponding coding structure.

(B) IDENTIFICATION OF CIVILIAN CYBER PERSONNEL.—Not later than 9 months after the date of enactment of this Act, the Director, in coordination with the Director of National Intelligence, shall establish procedures to implement the National Initiative for Cybersecurity Education's coding structure to identify all Federal civilian positions that require the performance of information technology, cybersecurity, or other cyber-related functions.

(C) IDENTIFICATION OF NON-CIVILIAN CYBER PERSONNEL.—Not later than 18 months after the date of enactment of this Act, the Secretary of Defense shall establish procedures to implement the National Initiative for Cybersecurity Education's coding structure to identify all Federal non-civilian positions that require the performance of information technology, cybersecurity or other cyber-related functions.

(D) BASELINE ASSESSMENT OF EXISTING CYBERSECURITY WORKFORCE.—Not later than 3 months after the date on which the procedures are developed under subparagraphs (B) and (C), respectively, the head of each Federal agency shall submit to the appropriate congressional committees of jurisdiction a report that identifies—

(i) the percentage of personnel with information technology, cybersecurity, or other cyber-related job functions who currently hold the appropriate industry-recognized certifications as identified in the National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework;

(ii) the level of preparedness of other civilian and non-civilian cyber personnel without existing credentials to pass certification exams; and

(iii) a strategy for mitigating any gaps identified in clause (i) or (ii) with the appropriate training and certification for existing personnel.

(E) PROCEDURES FOR ASSIGNING CODES.—Not later than 3 months after the date on which the procedures are developed under subparagraphs (B) and (C), respectively, the head of each Federal agency shall establish procedures—

(i) to identify all encumbered and vacant positions with information technology, cybersecurity, or other cyber-related functions

(as defined in the National Initiative for Cybersecurity Education's coding structure); and

(ii) to assign the appropriate employment code to each such position, using agreed standards and definitions.

(2) CODE ASSIGNMENTS.—Not later than 1 year after the date after the procedures are established under paragraph (1)(E), the head of each Federal agency shall complete assignment of the appropriate employment code to each position within the agency with information technology, cybersecurity, or other cyber-related functions.

(c) PROGRESS REPORT.—Not later than 180 days after the date of enactment of this Act, the Director shall submit a progress report on the implementation of this section to the appropriate congressional committees.

SEC. 204. IDENTIFICATION OF CYBER-RELATED ROLES OF CRITICAL NEED.

(a) IN GENERAL.—Beginning not later than 1 year after the date on which the employment codes are assigned to employees pursuant to section 203(b)(2), and annually through 2022, the head of each Federal agency, in consultation with the Director and the Secretary of Homeland Security, shall—

(1) identify information technology, cybersecurity, or other cyber-related roles of critical need in the agency's workforce; and

(2) submit a report to the Director that—

(A) describes the information technology, cybersecurity, or other cyber-related roles identified under paragraph (1); and

(B) substantiates the critical need designations.

(b) GUIDANCE.—The Director shall provide Federal agencies with timely guidance for identifying information technology, cybersecurity, or other cyber-related roles of critical need, including—

(1) current information technology, cybersecurity, and other cyber-related roles with acute skill shortages; and

(2) information technology, cybersecurity, or other cyber-related roles with emerging skill shortages.

(c) CYBERSECURITY NEEDS REPORT.—Not later than 2 years after the date of the enactment of this Act, the Director, in consultation with the Secretary of Homeland Security, shall—

(1) identify critical needs for information technology, cybersecurity, or other cyber-related workforce across all Federal agencies; and

(2) submit a progress report on the implementation of this section to the appropriate congressional committees.

SEC. 205. GOVERNMENT ACCOUNTABILITY OFFICE STATUS REPORTS.

The Comptroller General of the United States shall—

(1) analyze and monitor the implementation of sections 203 and 204; and

(2) not later than 3 years after the date of the enactment of this Act, submit a report to the appropriate congressional committees that describes the status of such implementation.

SA 2559. Mr. MANCHIN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 8, between lines 23 and 24, insert the following:

(16) REAL TIME; REAL-TIME.—The terms ''real time'' and ''real-time'' means as close to real time as practicable.

(17) DELAY.—The term ''delay'', with respect to the sharing of a cyber threat indicator, excludes any time necessary to ensure that the cyber threat indicator shared does not contain any personally identifiable information not needed to describe or identify a cybersecurity threat.

(18) MODIFICATION.—The term ''modification'', with respect to the sharing of a cyber threat indicator, excludes any process necessary to ensure that the cyber threat indicator modified does not contain any personally identifiable information not needed to describe or identify a cybersecurity threat.

SA 2560. Mr. MANCHIN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 15, strike lines 4 through 10, and insert the following:

(1) IN GENERAL.—

(A) AUTHORIZATION.—Except as provided in subparagraph (B) and paragraph (2) and notwithstanding any other provision of law, an entity may, for the purposes permitted under this Act 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.

(B) EXCEPTION FOR DEPARTMENT OF DEFENSE.—Notwithstanding subparagraph (A), no entity is permitted under this Act to share with the Department of Defense or any component of the Department, including the National Security Agency, a cyber threat indicator or defensive measure.

SA 2561. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

TITLE ____—CARRYING OF FIREARMS ON MILITARY INSTALLATIONS

SEC. _____1. SHORT TITLE.

This title may be cited as the ''Servicemembers Self-Defense Act of 2015''.

SEC. _____2. FIREARMS PERMITTED ON DEPARTMENT OF DEFENSE PROPERTY.

Section 930(g)(1) of title 18, United States Code, is amended—

(1) by striking ''The term 'Federal facility' means'' and inserting the following: ''The term 'Federal facility'—

''(A) means'';

(2) by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following:

''(B) with respect to a qualified member of the Armed Forces, as defined in section 926D(a), does not include any land, a building, or any part thereof owned or leased by the Department of Defense.''.

SEC. _____3. LAWFUL POSSESSION OF FIREARMS ON MILITARY INSTALLATIONS BY MEMBERS OF THE ARMED FORCES.

(a) MODIFICATION OF GENERAL ARTICLE.—Section 934 of title 10, United States Code (article 134 of the Uniform Code of Military Justice), is amended—

(1) by inserting ''(a) IN GENERAL.—'' before ''Though not specifically mentioned''; and

(2) by adding at the end the following new subsection:

''(b) POSSESSION OF A FIREARM.—The possession of a concealed or open carry firearm by a member of the armed forces subject to this chapter on a military installation, if lawful under the laws of the State in which the installation is located, is not an offense under this section.''.

(b) MODIFICATION OF REGULATIONS.—Not later than 30 days after the date of the enactment of this Act, the Secretary of Defense shall amend Department of Defense Directive number 5210.56 to provide that members of the Armed Forces may possess firearms for defensive purposes on facilities and installations of the Department of Defense in a manner consistent with the laws of the State in which the facility or installation concerned is located.

SEC. _____4. CARRYING OF CONCEALED FIREARMS BY QUALIFIED MEMBERS OF THE ARMED FORCES.

(a) IN GENERAL.—Chapter 44 of title 18, United States Code, is amended by inserting after section 926C the following

''§ 926D. Carrying of concealed firearms by qualified members of the Armed Forces

''(a) DEFINITIONS.—As used in this section—

''(1) the term 'firearm'—

''(A) except as provided in this paragraph, has the same meaning as in section 921;

''(B) includes ammunition not expressly prohibited by Federal law or subject to the provisions of the National Firearms Act; and

''(C) does not include—

''(i) any machinegun (as defined in section 5845 of the National Firearms Act);

''(ii) any firearm silencer; or

''(iii) any destructive device; and

''(2) the term 'qualified member of the Armed Forces' means an individual who—

''(A) is a member of the Armed Forces on active duty status, as defined in section 101(d)(1) of title 10;

''(B) is not the subject of disciplinary action under the Uniform Code of Military Justice;

''(C) is not under the influence of alcohol or another intoxicating or hallucinatory drug or substance; and

''(D) is not prohibited by Federal law from receiving a firearm.

''(b) AUTHORIZATION.—Notwithstanding any provision of the law of any State or any political subdivision thereof, an individual who is a qualified member of the Armed Forces and who is carry identification required by subsection (d) may carry a concealed firearm that has been shipped or transported in interstate or foreign commerce, subject to subsection (c).

''(c) LIMITATIONS.—This section shall not be construed to superseded or limit the laws of any State that—

''(1) permit private persons or entities to prohibit or restrict the possession of concealed firearms on their property; or

''(2) prohibit or restrict the possession of firearms on any State or local government property, installation, building, base, or park.

''(d) IDENTIFICATION.—The identification required by this subsection is the photographic identification issued by the Department of Defense for the qualified member of the Armed Forces.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 44 of title 18, United States Code, is amended by inserting after the item relating to section 926C the following:

''926D. Carrying of concealed firearms by qualified members of the Armed Forces.''.

SA 2562. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about

cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end of the bill, add the following:

SEC. 11. LIMITATION ON FEDERAL FUNDS TO SANCTUARY CITIES.

(a) IN GENERAL.—Section 642 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1373) is amended by adding at the end the following:

''(d) LIMITATION ON FEDERAL FUNDS TO SANCTUARY CITIES.—

''(1) SANCTUARY CITY DEFINED.—In this section, the term 'sanctuary city' means a State or subdivision of a State that the Attorney General determines—

''(A) has in effect a statute, policy, or practice that is not in compliance with subsection (a) or (b); or

''(B) does not have a statute, policy, or practice that requires law enforcement officers—

''(i) to notify the U.S. Immigration and Customs Enforcement if the State or unit has custody of an alien without lawful status in the United States and detain the alien for no more than six hours for no other purpose than to determine whether or not U.S. Immigration and Customs Enforcement will issue a detainer request; and

''(ii) to maintain custody of such an alien for a period of not less than 48 hours (excluding Saturdays, Sundays, and holidays) if U.S. Immigration and Customs Enforcement issues a detainer for such alien.

''(2) LIMITATION ON GRANTS.—A sanctuary city shall not be eligible to receive, for a minimum period of at least 1 year, any funds pursuant to—

''(A) the Edward Byrne Memorial Justice Assistance Grant Program established pursuant to subpart 1 of part E of title I of the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. 3750 et seq.);

''(B) the 'Cops' program under part Q of title I of the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. 3796dd et seq.);

''(C) the Urban Area Security Initiative authorized under section 2003 of the Homeland Security Act of 2002 (6 U.S.C. 604);

''(D) the State Homeland Security Grant Program authorized under section 2004 of the Homeland Security Act of 2002 (6 U.S.C. 605);

''(E) the port security grant program authorized under section 70107 of title 46, United States Code;

''(F) the State Criminal Alien Assistance Program under section 241(i) of the Immigration and Nationality Act (8 U.S.C. 1231(i)); or

''(G) any other non-disaster preparedness grant program administered by the Federal Emergency Management Agency.

''(3) TERMINATION OF INELIGIBILITY.—A jurisdiction that is found to be a sanctuary city shall only become eligible to receive funds under a program set out under paragraph (1) after the Attorney General certifies that the jurisdiction is no longer a sanctuary city.''.

(b) CLERICAL AMENDMENTS.—Section 642 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1373) is amended by striking ''Immigration and Naturalization Service'' each place that term appears and inserting ''Department of Homeland Security''.

SEC. 12. TRANSFER OF ALIENS FROM BUREAU OF PRISONS CUSTODY.

(a) TRANSFER TO U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT.—The Attorney General shall prioritize a request from the Secretary of Homeland Security to transfer a covered alien to the custody of U.S. Immigration and Customs Enforcement before a request from the appropriate official of a State or a subdivision of a State to transfer the covered alien to the custody of such State or subdivision.

(b) COVERED ALIEN DEFINED.—In this section, the term ''covered alien'' means an alien who—

(1) is without lawful status in the United States; and

(2) is in the custody of the Bureau of Prisons.

SA 2563. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

TITLE _____—FEDERAL RESERVE TRANSPARENCY

SEC. __01. SHORT TITLE.

This title may be cited as the ''Federal Reserve Transparency Act of 2015''.

SEC. __02. AUDIT REFORM AND TRANSPARENCY FOR THE BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM.

(a) IN GENERAL.—Notwithstanding section 714 of title 31, United States Code, or any other provision of law, an audit of the Board of Governors of the Federal Reserve System and the Federal reserve banks under subsection (b) of such section 714 shall be completed within 12 months of the date of enactment of this Act.

(b) REPORT.—

(1) IN GENERAL.—A report on the audit required under subsection (a) shall be submitted by the Comptroller General to the Congress before the end of the 90-day period beginning on the date on which such audit is completed and made available to the Speaker of the House, the majority and minority leaders of the House of Representatives, the majority and minority leaders of the Senate, the Chairman and Ranking Member of the committee and each subcommittee of jurisdiction in the House of Representatives and the Senate, and any other Member of Congress who requests it.

(2) CONTENTS.—The report under paragraph (1) shall include a detailed description of the findings and conclusion of the Comptroller General with respect to the audit that is the subject of the report, together with such recommendations for legislative or administrative action as the Comptroller General may determine to be appropriate.

(c) REPEAL OF CERTAIN LIMITATIONS.—Subsection (b) of section 714 of title 31, United States Code, is amended by striking all after ''in writing.''.

(d) TECHNICAL AND CONFORMING AMENDMENT.—Section 714 of title 31, United States Code, is amended by striking subsection (f).

SEC. __03. AUDIT OF LOAN FILE REVIEWS REQUIRED BY ENFORCEMENT ACTIONS.

(a) IN GENERAL.—The Comptroller General of the United States shall conduct an audit of the review of loan files of homeowners in foreclosure in 2009 or 2010, required as part of the enforcement actions taken by the Board of Governors of the Federal Reserve System against supervised financial institutions.

(b) CONTENT OF AUDIT.—The audit carried out pursuant to subsection (a) shall consider, at a minimum—

(1) the guidance given by the Board of Governors of the Federal Reserve System to independent consultants retained by the supervised financial institutions regarding the procedures to be followed in conducting the file reviews;

(2) the factors considered by independent consultants when evaluating loan files;

(3) the results obtained by the independent consultants pursuant to those reviews;

(4) the determinations made by the independent consultants regarding the nature and extent of financial injury sustained by each homeowner as well as the level and type of remediation offered to each homeowner; and

(5) the specific measures taken by the independent consultants to verify, confirm, or rebut the assertions and representations made by supervised financial institutions regarding the contents of loan files and the extent of financial injury to homeowners.

(c) REPORT.—Not later than the end of the 6-month period beginning on the date of the enactment of this Act, the Comptroller General shall issue a report to the Congress containing all findings and determinations made in carrying out the audit required under subsection (a).

SA 2564. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 38, line between lines 19 and 20, insert the following:

(d) EXCEPTION.—This section shall not apply to any private entity that, in the course of monitoring information under section 4(a) or sharing information under section 4(c), breaks a user agreement or privacy agreement with a customer of the private entity.

SA 2565. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 40, between lines 23 and 24, insert the following:

(iv) For inclusion in the unclassified form of this report under paragraph (4) of this subsection, to the greatest extent practicable, the number of United States persons who have been the subject of monitoring authorized under section 4.

(v) For inclusion in the unclassified form of this report under paragraph (4) of this subsection, to the greatest extent practicable, the number of United States persons with respect to whom personal information of or identifying the persons was shared with a Federal entity under this Act.

SA 2566. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 11, line 19, insert ''with an entity or another Federal entity'' after ''indicator''.

SA 2567. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end of section 8, add the following:

(n) PRESERVATION OF PRIVACY LAW.—Notwithstanding any other provision of this Act, nothing in this Act shall supersede any provision of law as it relates to the retention by a Federal entity of personal information of or identifying a specific United States person.

SA 2568. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 45, line 4, add ''Nothing in this Act shall be construed to prohibit or limit the disclosure of such information to the Privacy and Civil Liberties Oversight Board.'' after ''law.''.

SA 2569. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. RULE OF CONSTRUCTION.

Nothing in this Act or amendments made by this Act shall be construed as permitting the Federal Government to access communications content outside of networks of the Federal Government, including e-mail and messaging content, of a person located in the United States without prior court approval.

SA 2570. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. FOURTH AMENDMENT PRESERVATION AND PROTECTION.

(a) SHORT TITLE.—This section may be cited as the ''Fourth Amendment Preservation and Protection Act of 2015''.

(b) FINDINGS.—Congress finds that the right under the Fourth Amendment to the Constitution of the United States of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures is violated when the Federal Government or a State or local government acquires information voluntarily relinquished by a person to another party for a limited business purpose without the express informed consent of the person to the specific request by the Federal Government or a State or local government or a warrant, upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

(c) DEFINITION.—In this section, the term ''system of records'' means any group of records from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular associated with the individual.

(d) PROHIBITION.—

(1) IN GENERAL.—Except as provided in paragraph (2), the Federal Government and a State or local government may not obtain or seek to obtain information relating to an individual or group of individuals held by a third party in a system of records, and no such information shall be admissible in a criminal prosecution in a court of law.

(2) EXCEPTION.—The Federal Government or a State or local government may obtain, and a court may admit, information relating to an individual held by a third party in a system of records if—

(A) the individual whose name or identification information the Federal Government or State or local government is using to access the information provides express and informed consent to the search; or

(B) the Federal Government or State or local government obtains a warrant, upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

SA 2571. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. CLARIFICATION ON PROHIBITION ON SEARCHING OF COLLECTIONS OF COMMUNICATIONS TO CONDUCT WARRANTLESS SEARCHES FOR THE COMMUNICATIONS OF UNITED STATES PERSONS.

Section 702(b) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(b)) is amended—

(1) by redesignating paragraphs (1) through (5) as subparagraphs (A) through (E), respectively, and indenting such subparagraphs, as so redesignated, an additional two ems from the left margin;

(2) by striking ''An acquisition'' and inserting the following:

''(1) IN GENERAL.—An acquisition''; and

(3) by adding at the end the following:

''(2) CLARIFICATION ON PROHIBITION ON SEARCHING OF COLLECTIONS OF COMMUNICATIONS OF UNITED STATES PERSONS.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), no officer or employee of the United States may conduct a search of a collection of communications acquired under this section in an effort to find communications of a particular United States person (other than a corporation).

''(B) CONCURRENT AUTHORIZATION AND EXCEPTION FOR EMERGENCY SITUATIONS.—Subparagraph (A) shall not apply to a search for communications related to a particular United States person if—

''(i) such United States person is the subject of an order or emergency authorization authorizing electronic surveillance or physical search under section 105, 304, 703, 704, or 705 of this Act, or under title 18, United States Code, for the effective period of that order;

''(ii) the entity carrying out the search has a reasonable belief that the life or safety of such United States person is threatened and the information is sought for the purpose of assisting that person; or

''(iii) such United States person has consented to the search.''.

SA 2572. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ____. PROHIBITION ON DATA SECURITY VULNERABILITY MANDATES.

(a) IN GENERAL.—Except as provided in subsection (b), no agency may mandate that a manufacturer, developer, or seller of covered products design or alter the security functions in its product or service to allow the surveillance of any user of such product or service, or to allow the physical search of such product, by any agency.

(b) EXCEPTION.—Subsection (a) shall not apply to mandates authorized under the Communications Assistance for Law Enforcement Act (47 U.S.C. 1001 et seq.).

(c) COVERED PRODUCT DEFINED.—In this section, the term ''covered product'' means any computer hardware, computer software, or electronic device that is made available to the general public.

SA 2573. Mr. FLAKE submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. CRITICAL ELECTRIC INFRASTRUCTURE SECURITY.

(a) IN GENERAL.—Part II of the Federal Power Act is amended by inserting after section 215 (16 U.S.C. 824o) the following:

''SEC. 215A. CRITICAL ELECTRIC INFRASTRUCTURE SECURITY.

''(a) DEFINITIONS.—In this section:

''(1) BULK-POWER SYSTEM; ELECTRIC RELIABILITY ORGANIZATION; REGIONAL ENTITY.—The terms 'bulk-power system', 'Electric Reliability Organization', and 'regional entity' have the meanings given those terms in section 215.

''(2) CRITICAL ELECTRIC INFRASTRUCTURE.—The term 'critical electric infrastructure' means a system or asset of the bulk-power system, whether physical or virtual, the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of those matters.

''(3) CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—

''(A) IN GENERAL.—The term 'critical electric infrastructure information' means information related to critical electric infrastructure, or proposed critical electric infrastructure, generated by or provided to the Commission or other Federal agency, other than classified national security information, that is designated as critical electric infrastructure information by the Commission under subsection (c)(2).

''(B) INCLUSIONS.—The term 'critical electric infrastructure information' includes information that qualifies as critical energy infrastructure information under regulations promulgated by the Commission.

''(4) CYBERSECURITY THREAT.—The term ''cybersecurity threat' means the imminent danger of an act that severely disrupts, attempts to severely disrupt, or poses a significant risk of severely disrupting the operation of programmable electronic devices or communications networks (including hardware, software, and data) essential to the reliable operation of the bulk-power system.

''(5) ELECTROMAGNETIC PULSE.—The term 'electromagnetic pulse' means 1 or more pulses of electromagnetic energy emitted by

a device capable of disabling or disrupting operation of, or destroying, electronic devices or communications networks, including hardware, software, and data, by means of such a pulse.

''(6) GEOMAGNETIC STORM.—The term 'geomagnetic storm' means a temporary disturbance of the magnetic field of the Earth resulting from solar activity.

''(7) GRID SECURITY EMERGENCY.—The term 'grid security emergency' means the imminent danger of—

''(A) a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event, that could disrupt the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of the bulk-power system; and

''(B) disruption of the operation of such devices or networks, with significant adverse effects on the reliability of the bulk-power system, as a result of such act or event.

''(8) SECRETARY.—The term 'Secretary' means the Secretary of Energy.

''(b) AUTHORITY TO ADDRESS GRID SECURITY EMERGENCY.—

''(1) AUTHORITY.—

''(A) IN GENERAL.—If the President issues and provides to the Secretary a written directive or determination identifying a cybersecurity threat or grid security emergency, the Secretary may, with or without notice, hearing, or report, issue such orders for emergency measures as are necessary in the judgment of the Secretary to protect the bulk-power system during the cybersecurity threat or grid security emergency.

''(B) RULES.—As soon as practicable but not later than 180 days after the date of enactment of this section, the Secretary shall, after notice and opportunity for comment, establish rules of procedure that ensure that the authority described in subparagraph (A) can be exercised expeditiously.

''(2) NOTIFICATION OF CONGRESS.—If the President issues and provides to the Secretary a written directive or determination under paragraph (1), the President shall promptly notify congressional committees of relevant jurisdiction, including the Committee on Energy and Commerce of the House of Representatives and the Committee on Energy and Natural Resources of the Senate, of the contents of, and justification for, the directive or determination.

''(3) CONSULTATION.—Before issuing an order for emergency measures under paragraph (1), the Secretary shall, to the extent practicable in light of the nature of the cybersecurity threat or grid security emergency and the urgency of the need for action, consult with appropriate governmental authorities in Canada and Mexico, entities described in paragraph (4), the Commission, and other appropriate Federal agencies regarding implementation of the emergency measures.

''(4) APPLICATION.—An order for emergency measures under this subsection may apply to—

''(A) the Electric Reliability Organization;

''(B) a regional entity; or

''(C) any owner, user, or operator of the bulk-power system.

''(5) EXPIRATION AND REISSUANCE.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), an order for emergency measures issued under paragraph (1) shall expire not later than 30 days after the issuance of the order.

''(B) EXTENSIONS.—The Secretary may reissue an order for emergency measures issued under paragraph (1) for subsequent periods, not to exceed 30 days for each such period, if the President, for each such period, issues and provides to the Secretary a written directive or determination that the cybersecurity threat or grid security emergency identified under paragraph (1) continues to exist or that the emergency measure continues to be required.

''(6) COST RECOVERY FOR CRITICAL ELECTRIC INFRASTRUCTURE.—If the Commission determines that owners, operators, or users of the critical electric infrastructure have incurred substantial costs to comply with an order for emergency measures issued under this subsection and that such costs were prudently incurred and cannot reasonably be recovered through regulated rates or market prices for the electric energy or services sold by such owners, operators, or users, the Commission may, after notice and an opportunity for comment, prescribe standards for a public utility to seek to recover such costs by filing a rate schedule or tariff pursuant to section 205 for sales of electric energy or the transmission of electric energy subject to the jurisdiction of the Commission.

''(7) TEMPORARY ACCESS TO CLASSIFIED INFORMATION.—The Secretary, and other appropriate Federal agencies, shall, to the extent practicable and consistent with the obligations of the Secretary and Federal agencies to protect classified information, provide temporary access to classified information related to a cybersecurity threat or grid security emergency for which emergency measures are issued under paragraph (1) to key personnel of any entity subject to the emergency measures to enable optimum communication between the entity and the Secretary and other appropriate Federal agencies regarding the cybersecurity threat or grid security emergency.

''(c) PROTECTION AND SHARING OF CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—

''(1) PROTECTION OF CRITICAL ELECTRIC INFRASTRUCTURE.—Critical electric infrastructure information—

''(A) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code; and

''(B) shall not be made available by any State, political subdivision, or tribal authority pursuant to any State, political subdivision, or tribal law requiring disclosure of information or records.

''(2) DESIGNATION AND SHARING OF CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—Not later than 1 year after the date of enactment of this section, the Commission, in consultation with the Secretary, shall promulgate such regulations and issue such orders as necessary—

''(A) to designate critical electric infrastructure information;

''(B) to prohibit the unauthorized disclosure of critical electric infrastructure information; and

''(C) to ensure there are appropriate sanctions in place for Commissioners, officers, employees, or agents of the Commission who knowingly and willfully disclose critical electric infrastructure information in a manner that is not authorized under this section.

''(3) CONSIDERATIONS.—In promulgating regulations and issuing orders under paragraph (2), the Commission shall take into consideration the role of State commissions in—

''(A) reviewing the prudence and cost of investments;

''(B) determining the rates and terms of conditions for electric services; and

''(C) ensuring the safety and reliability of the bulk-power system and distribution facilities within the respective jurisdictions of the State commissions.

''(4) NO REQUIRED SHARING OF INFORMATION.—Nothing in this section requires a person or entity in possession of critical electric infrastructure information to share the information with Federal, State, local, or tribal authorities, or any other person or entity.

''(5) DISCLOSURE OF NONCRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—In carrying out this section, the Commission shall segregate critical electric infrastructure information within documents and electronic communications, wherever feasible, to facilitate disclosure of information that is not designated as critical electric infrastructure information.

''(d) SECURITY CLEARANCES.—

''(1) IN GENERAL.—The Secretary shall facilitate and, to the extent practicable, expedite the acquisition of adequate security clearances by key personnel of any entity subject to this section, to enable optimum communication with Federal agencies regarding threats to the security of the critical electric infrastructure.

''(2) SHARING.—The Secretary, the Commission, and other appropriate Federal agencies shall, to the extent practicable and consistent with the obligations of the Secretary, Commission, and Federal agencies to protect classified and critical electric infrastructure information, share timely actionable information regarding grid security with appropriate key personnel of owners, operators, and users of the critical electric infrastructure.

''(e) CLARIFICATIONS OF LIABILITY.—

''(1) IN GENERAL.—Except as provided in paragraph (3), to the extent any action or omission taken by an entity that is necessary to comply with an order for emergency measures issued under subsection (b)(1), including any action or omission taken to voluntarily comply with the order, results in noncompliance with, or causes the entity not to comply with, any rule, order, regulation, or provision of this Act, including any reliability standard approved by the Commission pursuant to section 215, the action or omission shall not be considered a violation of the rule, order, regulation, or provision.

''(2) RELATIONSHIP TO OTHER LAW.—Except as provided in paragraph (3), an action or omission taken by an owner, operator, or user of the bulk-power system to comply with an order for emergency measures issued under subsection (b)(1) shall be treated as an action or omission taken to comply with an order issued under section 202(c) for purposes of section 215.

''(3) ADMINISTRATION.—Nothing in this subsection requires dismissal of a cause of action against an entity that, in the course of complying with an order for emergency measures issued under subsection (b)(1) by taking an action or omission for which the entity would be liable but for paragraph (1) or (2), takes the action or omission in a grossly negligent manner.''.

(b) CONFORMING AMENDMENTS.—Section 201 of the Federal Power Act (16 U.S.C. 824) is amended by inserting ''215A,'' after ''215,'' each place it appears in subsections (b)(2) and (e).

SA 2574. Mr. HATCH submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE II—LAW ENFORCEMENT ACCESS TO DATA STORED ABROAD ACT

SEC. 201. SHORT TITLE.

This title may be cited as the ''The Law Enforcement Access to Data Stored Abroad Act''.

SEC. 202. FINDINGS.

Congress finds the following:

(1) The Electronic Communications Privacy Act of 1986 (Public Law 99–508; 100 Stat. 1848) (referred to in this section as ''ECPA'') was intended to protect the privacy of electronic communications stored with providers of electronic communications services and remote computing services, while balancing the legitimate needs of law enforcement to access records stored by such providers.

(2) To strike this balance, ECPA authorized governmental entities to obtain certain categories of communications data from providers using established, pre-existing forms of process—warrants and subpoenas. It also created a new form of court order, in section 2703(d) of title 18, United States Code, that governmental entities could use to obtain additional types of communications data.

(3) It has been well established that courts in the United States lack the power to issue warrants authorizing extraterritorial searches and seizures, and neither ECPA nor subsequent amendments extended the warrant power of courts in the United States beyond the territorial reach of the United States.

(4) Nevertheless, Congress also recognizes the legitimate needs of law enforcement agencies in the United States to obtain, through lawful process, electronic communications relevant to criminal investigations related to United States persons wherever that content may be stored. Therefore, this title authorizes the use of search warrants extraterritorially only where the Government seeks to obtain the contents of electronic communications belonging to a United States person.

SEC. 203. SCOPE AND CLARIFICATION OF WARRANT REQUIREMENT.

(a) IN GENERAL.—Chapter 121 of title 18, United States Code, is amended—

(1) in section 2702(a), by amending paragraph (3) to read as follows:

''(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge to any governmental entity the contents of any communication described in section 2703(a), or any record or other information pertaining to a subscriber or customer of such service.'';

(2) in section 2703—

(A) by striking subsections (a) and (b) and inserting the following:

''(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATION IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service or remote computing service of the contents of a wire or electronic communication that is in electronic storage with or otherwise stored, held, or maintained by the provider only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. Subject to subsection (b), a warrant issued pursuant to this subsection may be used to require the disclosure of contents of a wire or electronic communication that are in the provider's electronic storage within the United States or otherwise stored, held, or maintained within the United States by the provider.

''(b) WARRANT REQUIREMENTS.—A warrant issued under subsection (a) may require the disclosure of the contents of a wire or electronic communication, regardless of where such contents may be in electronic storage or otherwise stored, held, or maintained by the provider, if the account-holder whose contents are sought by the warrant is a United States person. A court issuing a warrant pursuant to this subsection, on a motion made promptly by the service provider, shall modify or vacate such warrant if the court finds that the warrant would require the provider of an electronic communications or remote computing service to violate the laws of a foreign country.'';

(B) in subsection (d), in the first sentence—

(i) by striking ''(b) or'';

(ii) by striking ''the contents of a wire or electronic communication, or''; and

(iii) by striking ''sought, are'' and inserting ''sought are''; and

(C) by adding at the end the following:

''(h) RULE OF CONSTRUCTION.—Nothing in this section or in section 2702 shall be construed to limit the authority of a governmental entity to use an administrative subpoena authorized under a Federal or State statute or to use a Federal or State grand jury, trial, or civil discovery subpoena to—

''(1) require an originator, addressee, or intended recipient of an electronic communication to disclose the contents of the electronic communication to the governmental entity; or

''(2) require an entity that provides electronic communication services to the officers, directors, employees, or agents of the entity (for the purpose of carrying out their duties) to disclose the contents of an electronic communication to or from an officer, director, employee, or agent of the entity to a governmental entity, if the electronic communication is held, stored, or maintained on an electronic communications system owned or operated by the entity.

''(i) NOTICE.—Except as provided in section 2705, not later than 10 business days after a governmental entity receives the contents of a wire or electronic communication of a subscriber or customer from a provider of electronic communication service or remote computing service under subsection (a), the governmental entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, as specified by the court issuing the warrant, the subscriber or customer—

''(1) a copy of the warrant; and

''(2) notice that informs the customer or subscriber—

''(A) of the nature of the law enforcement inquiry with reasonable specificity; and

''(B) that information maintained for the customer or subscriber by the provider of electronic communication service or remote computing service named in the process or request was supplied to, or requested by, the governmental entity.'';

(3) in section 2704(a)(1), by striking ''section 2703(b)(2)'' and inserting ''section 2703'';

(4) in section 2705—

(A) in subsection (a), by striking paragraph (1) and inserting the following:

''(1) A governmental entity that is seeking a warrant under section 2703 may include in the application for the warrant a request, which the court shall grant, for an order delaying the notification required under section 2703(i) for a period of not more than 90 days, if the court determines that there is reason to believe that notification of the existence of the warrant may have an adverse result described in paragraph (2) of this subsection.''; and

(B) in subsection (b), in the matter preceding paragraph (1), by striking ''under section 2703(b)(1)''; and

(5) in section 2711—

(A) in paragraph (3)(B) by striking ''warrants; and'' and inserting ''warrants'';

(B) in paragraph (4) by striking ''thereof.'' and inserting ''thereof; and''; and

(C) by adding at the end the following:

''(5) the term 'United States person' means a citizen or permanent resident alien of the United States, or an entity or organization organized under the laws of the United States or a State or political subdivision thereof.''.

SEC. 204. MUTUAL LEGAL ASSISTANCE TREATY REFORMS.

(a) MUTUAL LEGAL ASSISTANCE TREATY TRANSPARENCY AND EFFICIENCY.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Attorney General shall establish—

(A) a form for use by a foreign government filing a mutual legal assistance treaty request (referred to in this section as an ''MLAT request''), which shall—

(i) be made available on the website of the Department of Justice; and

(ii) require sufficient information and be susceptible for use by a foreign government to provide all the information necessary for the MLAT request; and

(B) an online docketing system for all MLAT requests, which shall allow a foreign government to track the status of an MLAT request filed by the foreign government.

(2) ANNUAL PUBLICATION.—Beginning not later than 1 year after the date of enactment of this Act, and each year thereafter, the Attorney General shall publish on the website of the Department of Justice statistics on—

(A)(i) the number of MLAT requests made by the Department of Justice to foreign governments for the purpose of obtaining the contents of an electronic communication or other information or records from a provider of electronic communications or remote computing services; and

(ii) the average length of time taken by foreign governments to process the MLAT requests described in clause (i); and

(B)(i) the number of MLAT requests made to the Department of Justice by foreign governments for the purpose of obtaining the contents of an electronic communication or other information or records from a provider of electronic communications or remote computing services; and

(ii) the average length of time taken by the Department of Justice to process the MLAT requests described in clause (i).

(3) NOTICE TO DEPARTMENT OF STATE.—The Attorney General shall notify the Secretary of State not later than 7 days after the date on which disclosure of electronic communications content to a foreign government is made pursuant to an MLAT request.

(b) PRESERVATION OF RECORDS.—The Attorney General may issue a request pursuant to section 2703(f) of title 18, United States Code, upon receipt of an MLAT request that appears to be facially valid.

(c) NOTIFICATION TO PROVIDER OF MLAT REQUEST.—When the Attorney General makes use of the process provided in section 2703 of title 18, United States Code, to obtain information from an electronic communications provider or a remote computing provider based on an MLAT request, the Attorney General shall notify that provider in writing that the request has been made pursuant to a mutual legal assistance treaty.

SEC. 205. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) data localization requirements imposed by foreign governments on data providers are—

(A) incompatible with the borderless nature of the Internet;

(B) an impediment to online innovation; and

(C) unnecessary to meet the needs of law enforcement; and

(2) the Department of Justice, the Department of State, and the United States Trade Representatives should pursue open data flow policies with foreign nations.

SA 2575. Ms. HIRONO submitted an amendment intended to be proposed by

her to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 38, strike lines 7, 8, and 9, and insert the following:

(A) the date on which the interim policies and procedures are submitted to Congress under section 5(a)(1) and guidelines are submitted to Congress under section 5(b)(1); or

---

SA 2576. Mr. MARKEY submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 51, strike line 8 and insert the following:

SEC. 10. CYBERSECURITY STANDARDS FOR MOTOR VEHICLES.

(a) IN GENERAL.—Chapter 301 of title 49, United States Code, is amended—

(1) in section 30102(a)—

(A) by redesignating paragraphs (4) through (11) as paragraphs (10) through (17), respectively;

(B) by redesignating paragraphs (1) through (3) as paragraphs (4) through (6), respectively;

(C) by inserting before paragraph (3), as redesignated, the following:

''(1) 'Administrator' means the Administrator of the National Highway Traffic Safety Administration;

''(2) 'Commission' means the Federal Trade Commission;

''(3) 'critical software systems' means software systems that can affect the driver's control of the vehicle movement;''; and

(D) by inserting after paragraph (6), as redesignated, the following:

''(7) 'driving data' include, but are not limited to, any electronic information collected about—

''(A) a vehicle's status, including, but not limited to, its location or speed; and

''(B) any owner, lessee, driver, or passenger of a vehicle;

''(8) 'entry points' include, but are not limited to, means by which—

''(A) driving data may be accessed, directly or indirectly; or

''(B) control signals may be sent or received either wirelessly or through wired connections;

''(9) 'hacking' means the unauthorized access to electronic controls or driving data, either wirelessly or through wired connections;''; and

(2) by adding at the end the following:

''§ 30129. Cybersecurity standards

''(a) CYBERSECURITY STANDARDS.—

''(1) REQUIREMENT.—All motor vehicles manufactured for sale in the United States on or after the date that is 2 years after the date on which final regulations are prescribed pursuant to section 10(b)(2) of the Cybersecurity Information Sharing Act of 2015 shall comply with the cybersecurity standards set forth in paragraphs (2) through (4).

''(2) PROTECTION AGAINST HACKING.—

''(A) IN GENERAL.—All entry points to the electronic systems of each motor vehicle manufactured for sale in the United States shall be equipped with reasonable measures to protect against hacking attacks.

''(B) ISOLATION MEASURES.—The measures referred to in subparagraph (A) shall incorporate isolation measures to separate critical software systems from noncritical software systems.

''(C) EVALUATION.—The measures referred to in subparagraphs (A) and (B) shall be evaluated for security vulnerabilities following best security practices, including appropriate applications of techniques such as penetration testing.

''(D) ADJUSTMENT.—The measures referred to in subparagraphs (A) and (B) shall be adjusted and updated based on the results of the evaluation described in subparagraph (C).

''(3) SECURITY OF COLLECTED INFORMATION.—All driving data collected by the electronic systems that are built into motor vehicles shall be reasonably secured to prevent unauthorized access—

''(A) while such data are stored onboard the vehicle;

''(B) while such data are in transit from the vehicle to another location; and

''(C) in any subsequent offboard storage or use.

''(4) DETECTION, REPORTING, AND RESPONDING TO HACKING.—Any motor vehicle that presents an entry point shall be equipped with capabilities to immediately detect, report, and stop attempts to intercept driving data or control the vehicle.

''(b) PENALTIES.—A person that violates this section is liable to the United States Government for a civil penalty of not more than $5,000 for each violation in accordance with section 30165.''.

(b) RULEMAKING.—

(1) IN GENERAL.—Not later than 18 months after the date of the enactment of this Act, the Administrator, after consultation with the Commission, shall issue a Notice of Proposed Rulemaking to carry out section 30129 of title 49, United States Code, as added by subsection (a).

(2) FINAL REGULATIONS.—Not later than 3 years after the date of the enactment of this Act, the Administrator, after consultation with the Commission, shall issue final regulations to carry out section 30129 of title 49, United States Code, as added by subsection (a).

(3) UPDATES.—Not later than 3 years after final regulations are issued pursuant to paragraph (2) and not less frequently than once every 3 years thereafter, the Administrator, after consultation with the Commission, shall—

(A) review the regulations issued pursuant to paragraph (2); and

(B) update such regulations, as necessary.

(c) CLERICAL AMENDMENT.—The table of sections for chapter 301 of title 49, United States Code, is amended by striking the item relating to section 30128 and inserting the following:

''30128. Vehicle rollover prevention and crash mitigation.

''30129. Cybersecurity standards.''.

(d) CONFORMING AMENDMENT.—Section 30165(a)(1) of title 49, United States Code, is amended by inserting ''30129,'' after ''30127,''.

SEC. 11. CYBER DASHBOARD.

(a) IN GENERAL.—Section 32302 of title 49, United States Code, is amended by inserting after subsection (b) the following:

''(c) CYBER DASHBOARD.—

''(1) IN GENERAL.—All motor vehicles manufactured for sale in the United States on or after the date that is 2 years after the date on which final regulations are prescribed pursuant to section 11(b)(2) of the Cybersecurity Information Sharing Act of 2015 shall display a 'cyber dashboard', as a component of the label required to be affixed to each motor vehicle under section 32908(b).

''(2) FEATURES.—The cyber dashboard required under paragraph (1) shall inform consumers, through an easy-to-understand, standardized graphic, about the extent to which the motor vehicle protects the cybersecurity and privacy of motor vehicle owners, lessees, drivers, and passengers beyond the minimum requirements set forth in section 30129 of this title and in section 27 of the Federal Trade Commission Act.''.

(b) RULEMAKING.—

(1) IN GENERAL.—Not later than 18 months after the date of the enactment of this Act, the Administrator, after consultation with the Commission, shall prescribe regulations for the cybersecurity and privacy information required to be displayed under section 32302(c) of title 49, United States Code, as added by subsection (a).

(2) FINAL REGULATIONS.—Not later than 3 years after the date of the enactment of this Act, the Administrator, after consultation with the Commission, shall issue final regulations to carry out section 32302 of title 49, United States Code, as added by subsection (a).

(3) UPDATES.—Not less frequently than once every 3 years, the Administrator, after consultation with the Commission, shall—

(A) review the regulations issued pursuant to paragraph (2); and

(B) update such regulations, as necessary.

SEC. 12. PRIVACY STANDARDS FOR MOTOR VEHICLES.

(a) IN GENERAL.—The Federal Trade Commission Act (15 U.S.C. 41 et seq.) is amended by inserting after section 26 (15 U.S.C. 57c–2) the following:

''SEC. 27. PRIVACY STANDARDS FOR MOTOR VEHICLES.

''(a) IN GENERAL.—All motor vehicles manufactured for sale in the United States on or after the date that is 2 years after the date on which final regulations are prescribed pursuant to subsection (e) shall comply with the features required under subsections (b) through (d).

''(b) TRANSPARENCY.—Each motor vehicle shall provide clear and conspicuous notice, in clear and plain language, to the owners or lessees of such vehicle of the collection, transmission, retention, and use of driving data collected from such motor vehicle.

''(c) CONSUMER CONTROL.—

''(1) IN GENERAL.—Subject to paragraphs (2) and (3), owners or lessees of motor vehicles shall be given the option of terminating the collection and retention of driving data.

''(2) ACCESS TO NAVIGATION TOOLS.—If a motor vehicle owner or lessee decides to terminate the collection and retention of driving data under paragraph (1), the owner or lessee shall not lose access to navigation tools or other features or capabilities, to the extent technically possible.

''(3) EXCEPTION.—Paragraph (1) shall not apply to driving data stored as part of the electronic data recorder system or other safety systems on-board the motor vehicle that are required for post-incident investigations, emissions history checks, crash avoidance or mitigation, or other regulatory compliance programs.

''(d) LIMITATION ON USE OF PERSONAL DRIVING INFORMATION.—

''(1) IN GENERAL.—A manufacturer (including an original equipment manufacturer) may not use any information collected by a motor vehicle for advertising or marketing purposes without affirmative express consent by the owner or lessee.

''(2) REQUESTS.—Consent requests under paragraph (1)—

''(A) shall be clear and conspicuous;

''(B) shall be made in clear and plain language; and

''(C) may not be a condition for the use of any nonmarketing feature, capability, or functionality of the motor vehicle.

''(e) ENFORCEMENT.—A violation of this section shall be treated as an unfair and deceptive act or practice in violation of a rule prescribed under section 18(a)(1)(B).''.

(b) RULEMAKING.—

(1) IN GENERAL.—Not later than 18 months after the date of the enactment of this Act, the Commission, after consultation with the Administrator of the National Highway Traffic Safety Administration (referred to in this subsection as the ''Administrator''), shall prescribe regulations, in accordance with section 553 of title 5, United States Code, to carry out section 27 of the Federal Trade Commission Act, as added by subsection (a).

(2) FINAL REGULATIONS.—Not later than 3 years after the date of the enactment of this Act, the Commission, after consultation with the Administrator, shall issue final regulations, in accordance with section 553 of title 5, United States Code, to carry out section 27 of the Federal Trade Commission Act, as added by subsection (a).

(3) UPDATES.—Not less frequently than once every 3 years, the Commission, after consultation with the Administrator, shall—

(A) review the regulations prescribed pursuant to paragraph (2); and

(B) update such regulations, as necessary.

SEC. 13. CONFORMING AMENDMENTS.

SA 2577. Mr. MARKEY submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 17, between lines 18 and 19, insert the following:

(B) PROHIBITION ON USE FOR PURPOSES OTHER THAN CYBERSECURITY PURPOSES.—A private entity may not use a cyber threat indicator or a defensive measure received under this section for any other purpose than as authorized in subparagraph (A), including for commercial, marketing, and sales purposes not authorized in subparagraph (A).

SA 2578. Mr. VITTER (for himself and Mr. TESTER) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. REVIEW AND UPDATE OF GUIDANCE REGARDING SECURITY CLEARANCES FOR CERTAIN SENATE EMPLOYEES.

(a) DEFINITIONS.—In this section—

(1) the term ''covered committee of the Senate'' means—

(A) the Committee on Armed Services of the Senate;

(B) the Committee on Foreign Relations of the Senate;

(C) the Subcommittee on Defense of the Committee on Appropriations of the Senate;

(D) the Subcommittee on State, Foreign Operations, and Related Programs of the Committee on Appropriations of the Senate;

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

(F) the Committee on the Judiciary of the Senate;

(2) the term ''covered Member of the Senate'' means a Member of the Senate who serves on a covered committee of the Senate; and

(3) the term ''Senate employee'' means an employee whose pay is disbursed by the Secretary of the Senate.

(b) REVIEW OF PROCEDURES.—

(1) IN GENERAL.—Not later than 60 days after the date of enactment of this Act, the Director of Senate Security, in coordination with the Director of National Intelligence and the Chairperson of the Suitability and Security Clearance Performance Accountability Council established under Executive Order 13467 (73 Fed. Reg. 38103), shall—

(A) conduct a review of whether procedures in effect enable 1 Senate employee designated by each covered Member of the Senate to obtain security clearances necessary for access to classified national security information, including top secret and sensitive compartmentalized information, if the Senate employee meets the criteria for such clearances; and

(B) if the Director of Senate Security, in coordination with the Director of National Intelligence and the Chairperson of the Suitability and Security Clearance Performance Accountability Council established under Executive Order 13467 (73 Fed. Reg. 38103), determines the procedures described in subparagraph (A) are inadequate, issue guidelines on the establishment and implementation of such procedures.

(2) REPORT.—Not later than 90 days after the date of enactment of this Act, the Director of Senate Security shall submit to each covered committee of the Senate a report regarding the review conducted under paragraph (1)(A) and guidance, if any, issued under paragraph (1)(B).

(c) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to alter—

(1) the rule of the Information Security Oversight Office implementing Standard Form 312, which Members of Congress sign in order to be permitted to access classified information;

(2) the requirement that Members of the Senate satisfy the ''need-to-know'' requirement to access classified information;

(3) the scope of the jurisdiction of any committee or subcommittee of the Senate; or

(4) the inherent authority of the executive branch of the Government, the Office of Senate Security, any Committee of the Senate, or the Department of Defense to determine recipients of all classified information.

SA 2579. Mr. VITTER submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. SMALL BUSINESS CYBER SECURITY OPERATIONS CENTER.

(a) FINDINGS.—Congress finds the following:

(1) The Federal Government has been hit by a barrage of high-profile cyber assaults over the past year, including the attacks on the Office of Personnel Management and the Department of State.

(2) These attacks exposed the most sensitive personal information of millions of Federal employees and their families.

(3) The President has instituted emergency procedures to immediately deploy so-called indicators, or tell-tale signs of cybercrime operations, into agency anti-malware tools.

(4) According to the Federal Bureau of Investigation, small business concerns have lost more than $1,000,000,000 during the period beginning October 2013 and ending June 2015 as a result of cyber corporate account takeover and business email fraud.

(5) The Federal Government leverages the creative genius of small business concerns across the country to accomplish its missions.

(6) The Federal Acquisition Regulations dictates that a percentage of all Federal Government acquisition be set aside for small business concerns.

(7) Over 90 percent of small business concerns use the Internet through the course of their activities to conduct business.

(8) Small business concerns tend to have weaker online security and do not have necessary funding for high-end encryption technology or staff expertise.

(9) Industry reports indicate that 30 percent of cyber attacks target small business concerns and of those businesses that are attacked, 59 percent have no contingency plan, while according to a First Data report, the average cost for a data breach at a small business concern is $36,000 and rising annually.

(10) A 2012 Verizon study shows that in 855 data breaches examined, 71 percent occurred in businesses with fewer than 100 employees.

(11) Small business concerns are increasingly attacked with data breaches and ransomware, where an attacker encrypts the businesses data until a ransom is paid to the attacker.

(12) It is imperative that small business concerns are provided improved secured guidance to limit negative impacts on the economy of the United States.

(13) There is a vast cyber threat facing the business sector of the United States, which poses a direct threat against the national security of the United States, the Department of Defense, private industry, and critical infrastructure components.

(14) The current layer of protection from cyber threats does not exist for small business concerns.

(b) DEFINITIONS.—In this section—

(1) the term ''Center'' means the Small Business Cyber Security Operations Center established under subsection (c);

(2) the term ''cyber lab'' means—

(A) a Joint Cyber Training Lab; and

(B) a facility that works in conjunction with the National Guard Cyber Teams;

(3) the term ''Secretary'' means the Secretary of Homeland Security; and

(4) the term ''small business concern'' has the meaning given that term under section 3 of the Small Business Act (15 U.S.C. 632).

(c) ESTABLISHMENT.—Not later than 1 year after the date of enactment of this Act, the Secretary shall begin carrying out a 3-year pilot program to establish a cybersecurity operations center for small business concerns, to be known as the Small Business Cyber Security Operations Center.

(d) PART OF EXISTING CENTER.—The Secretary shall establish the Center as part of and co-locate the Center with a center providing situational awareness information to businesses on the date of enactment of this Act.

(e) DUTIES.—The Center shall—

(1) work with cyber labs to provide realistic scenario based training to network managers and security personnel of small business concerns, including monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities;

(2) provide periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analysis of cyber threat indicators and information in possession of—

(A) the Federal Government;

(B) the Business Emergency Operations Center operated by the Federal Emergency Management Agency; and

(C) other technology and cyber research centers, as determined appropriate by the Secretary;

(3) collaborate with private industry, academia, and the Department of Defense to develop a secure business supply chain which is capable of adapting, evolving, and responding to emergent cybersecurity threats;

(4) review and develop the necessary tools to—

(A) facilitate security information flow and mitigation actions;

(B) provide cyber attack sensing, warning, and response services;

(5) place an emphasis on accessibility and relevance to small business concerns; and

(6) review the policy limitations and restrictions on information sharing relating to cybersecurity.

(f) AUTHORIZATION OF APPROPRIATIONS.—

(1) IN GENERAL.—There is authorized to be appropriated to carry out this section $2,000,000 for each of fiscal years 2016 through 2019, to remain available until expended.

(2) OFFSET.—Section 21(a)(4)(C)(vii) of the Small Business Act (15 U.S.C. 648(a)(4)(C)(vii)) is amended—

(A) in subclause (I), by striking ''and'' at the end;

(B) in subclause (II), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(III) $133,000,000 for each of fiscal years 2016 through 2019.''.

SA 2580. Mr. FLAKE submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

Beginning on page 46, strike line 10 and all that follows through page 47, line 12, and insert the following:

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

(4) to require the use of the capability and process within the Department of Homeland Security developed under section 5(c).

(g) PRESERVATION OF CONTRACTUAL OBLIGATIONS AND RIGHTS.—Nothing in this Act 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 Act shall be construed to permit the Federal Government—

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

(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 another entity; 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 or another entity.

SA 2581. Mr. COTTON submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 29, strike line 9 and insert the following:

authority regarding a cybersecurity threat; and

(iii) communications between a private entity and the Federal Bureau of Investigation or the United States Secret Service regarding a cybersecurity threat;

SA 2582. Mr. FLAKE (for himself and Mr. FRANKEN) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

SEC. 11. EFFECTIVE PERIOD.

(a) IN GENERAL.—Except as provided in subsection (b), this Act and the amendments made by this Act shall be in effect during the 6-year period beginning on the date of the enactment of this Act.

(b) EXCEPTION.—With respect to any action authorized by this Act or information obtained pursuant to an action authorized by this Act, which occurred before the date on which the provisions referred to in subsection (a) cease to have effect, the provisions of this Act shall continue in effect.

SA 2583. Ms. BALDWIN submitted an amendment intended to be proposed by her to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

In section 7(a)(2), by striking subparagraph (F) and inserting the following:

(F) A review of actions taken by the Federal Government based on cyber threat indicators shared with the Federal Government under this Act, including—

(i) the number of actions taken by each agency, department, or component of the Federal Government with which the cyber threat indicators were shared;

(ii) the specific purpose under section 5(d)(5)(A) for which the cyber threat indicators were disclosed to, retained by, or used by each agency, department, or component of the Federal Government; and

(iii) the appropriateness of any subsequent retention, use, or dissemination of such cyber threat indicators by a Federal entity under section 5.

In section 7(b)(2)(B), by striking clause (ii) and inserting the following:

(ii) A review of the actions taken by Federal entities as a result of the receipt of such cyber threat indicators, including the number of actions taken by each Federal entity and the specific purpose under section 5(d)(5)(A) for which cyber threat indicators were disclosed to, retained by, or used by each Federal entity.

SA 2584. Mr. BLUMENTHAL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 44, between lines 5 and 6, insert the following:

(c) PRIVATE RIGHT OF ACTION FOR VIOLATIONS BY FEDERAL ENTITIES OF RESTRICTIONS ON DISCLOSURE, USE, AND PROTECTION OF VOLUNTARILY SHARED CYBER THREAT INDICATORS.—

(1) IN GENERAL.—If a department or agency of the Federal Government knowingly or recklessly violates the requirements of this Act with respect to the disclosure, use, or protection of voluntarily shared cyber threat indicators, the United States shall be liable to a person adversely affected by such violation in an amount equal to the sum of—

(A) the actual damages sustained by the person as a result of the violation or $50,000, whichever is greater; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

(2) VENUE.—An action to enforce liability created under this subsection may be brought in the district court of the United States in—

(A) the district in which the complainant resides;

(B) the district in which the principal place of business of the complainant is located;

(C) the district in which the department or agency of the Federal Government that disclosed the information is located; or

(D) the District of Columbia.

(3) STATUTE OF LIMITATIONS.—No action shall lie under this subsection unless such action is commenced not later than two years after the person adversely affected by a violation described in paragraph (1) first learns, or by which such person reasonably should have learned, of the facts and circumstances giving rise to the action.

SA 2585. Mr. BLUMENTHAL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 44, between lines 5 and 6, insert the following:

(c) PRIVATE RIGHT OF ACTION FOR VIOLATIONS BY FEDERAL ENTITIES OF RESTRICTIONS ON DISCLOSURE, USE, AND PROTECTION OF VOLUNTARILY SHARED CYBER THREAT INDICATORS.—

(1) IN GENERAL.—If a department or agency of the Federal Government knowingly or recklessly violates the requirements of this Act with respect to the disclosure, use, or protection of voluntarily shared cyber threat indicators, the United States shall be liable to a person adversely affected by such violation in an amount equal to the sum of—

(A) the actual damages sustained by the person as a result of the violation or $1,000, whichever is greater; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

(2) VENUE.—An action to enforce liability created under this subsection may be brought in the district court of the United States in—

(A) the district in which the complainant resides;

(B) the district in which the principal place of business of the complainant is located;

(C) the district in which the department or agency of the Federal Government that disclosed the information is located; or

(D) the District of Columbia.

(3) STATUTE OF LIMITATIONS.—No action shall lie under this subsection unless such action is commenced not later than two years after the person adversely affected by a violation described in paragraph (1) first learns, or by which such person reasonably should have learned, of the facts and circumstances giving rise to the action.

SA 2586. Mr. HEINRICH (for himself and Ms. HIRONO) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 51, strike lines 9 through 19.

SA 2587. Mr. LEAHY submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

Beginning on page 32, strike line 17 and all that follows through page 33, line 5.

SA 2588. Mrs. BOXER submitted an amendment intended to be proposed by her to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end of section 7, insert the following:

(c) ANNUAL DATA SECURITY CERTIFICATION.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act and not less frequently than annually thereafter, the Director of the Office of Management and Budget shall certify the adequacy of the security controls utilized by Federal entities to protect information shared or received under this Act.

(2) CONTENTS.—Each certificate issued by the Director under paragraph (1) shall include a description of the adequacy of the security controls of each Federal entity based on—

(A) a review of the annual reports and evaluations submitted under sections 3554(c) and 3555 of title 44, United States Code; and

(B) any additional certification requirements determined necessary by the Director.

(3) ACTIONS IF INADEQUATE SECURITY CONTROLS ARE DETECTED.—

(A) IN GENERAL.—If the Director determines the security controls of a Federal entity are not adequate to protect the information shared or received under this Act, the Director shall submit to such Federal entity, in writing, a notice of the actions the Federal entity shall take in order to ensure that the information is adequately protected.

(B) SCHEDULE AND EXPLANATION.—Not later than 30 days after the date the Director submits a notice under subparagraph (A), the Federal entity shall—

(i) take the actions required by the notice; or

(ii) submit to the Director and the appropriate committees of Congress, in writing, an explanation of why such actions have not been taken and an estimate of the number of days until such actions shall be taken.

(C) APPROPRIATE COMMITTEES OF CONGRESS.—In this paragraph, the term ''appropriate committees of Congress'' means the following:

(i) The Committee on Commerce, Science, and Transportation, the Committee on Homeland Security and Governmental Affairs, and the Select Committee on Intelligence of the Senate.

(ii) The Committee on Homeland Security, the Permanent Select Committee on Intelligence, the Committee on Oversight and Government Reform, and the Committee on Science, Space, and Technology of the House of Representatives.

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

SA 2589. Mr. MURPHY (for himself and Mr. HATCH) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

SEC. ____. JUDICIAL REDRESS.

(a) SHORT TITLE.—This section may be cited as the ''Judicial Redress Act of 2015''.

(b) EXTENSION OF PRIVACY ACT REMEDIES TO CITIZENS OF DESIGNATED COUNTRIES.—

(1) CIVIL ACTION; CIVIL REMEDIES.—With respect to covered records, a covered person may bring a civil action against an agency and obtain civil remedies, in the same manner, to the same extent, and subject to the same limitations, including exemptions and exceptions, as an individual may bring and obtain with respect to records under—

(A) section 552a(g)(1)(D) of title 5, United States Code, but only with respect to disclosures intentionally or willfully made in violation of section 552a(b) of such title; and

(B) subparagraphs (A) and (B) of section 552a(g)(1) of title 5, United States Code, but such an action may only be brought against a designated Federal agency or component.

(2) EXCLUSIVE REMEDIES.—The remedies set forth in paragraph (1) are the exclusive remedies available to a covered person under this subsection.

(3) APPLICATION OF THE PRIVACY ACT WITH RESPECT TO A COVERED PERSON.—For purposes of a civil action described in paragraph (1), a covered person shall have the same rights, and be subject to the same limitations, including exemptions and exceptions, as an individual has and is subject to under section 552a of title 5, United States Code, when pursuing the civil remedies described in subparagraphs (A) and (B) of paragraph (1).

(4) DESIGNATION OF COVERED COUNTRY.—

(A) IN GENERAL.—The Attorney General may, with the concurrence of the Secretary of State, the Secretary of the Treasury, and the Secretary of Homeland Security, designate a foreign country or regional economic integration organization, or member country of such organization, as a ''covered country'' for purposes of this subsection if—

(i) the country or regional economic integration organization, or member country of such organization, has entered into an agreement with the United States that provides for appropriate privacy protections for information shared for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses; or

(ii) the Attorney General has determined that the country or regional economic integration organization, or member country of such organization, has effectively shared information with the United States for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses and has appropriate privacy protections for such shared information.

(B) REMOVAL OF DESIGNATION.—The Attorney General may, with the concurrence of the Secretary of State, the Secretary of the Treasury, and the Secretary of Homeland Security, revoke the designation of a foreign country or regional economic integration organization, or member country of such organization, as a ''covered country'' if the Attorney General determines that such designated ''covered country''—

(i) is not complying with the agreement described under subparagraph (A)(i);

(ii) no longer meets the requirements for designation under subparagraph (A)(ii); or

(iii) impedes the transfer of information (for purposes of reporting or preventing unlawful activity) to the United States by a private entity or person.

(5) DESIGNATION OF DESIGNATED FEDERAL AGENCY OR COMPONENT.—

(A) IN GENERAL.—The Attorney General shall determine whether an agency or component thereof is a ''designated Federal agency or component'' for purposes of this subsection. The Attorney General shall not designate any agency or component thereof other than the Department of Justice or a component of the Department of Justice without the concurrence of the head of the relevant agency, or of the agency to which the component belongs.

(B) REQUIREMENTS FOR DESIGNATION.—The Attorney General may determine that an agency or component of an agency is a ''designated Federal agency or component'' for purposes of this subsection, if—

(i) the Attorney General determines that information exchanged by such agency with a covered country is within the scope of an agreement referred to in paragraph (4)(A)(i); or

(ii) with respect to a country or regional economic integration organization, or member country of such organization, that has been designated as a ''covered country'' under paragraph (4)(A)(ii), the Attorney General determines that designating such agency or component thereof is in the law enforcement interests of the United States.

(6) FEDERAL REGISTER REQUIREMENT; NONREVIEWABLE DETERMINATION.—The Attorney General shall publish each determination made under paragraphs (4) and (5). Such determination shall not be subject to judicial or administrative review.

(7) JURISDICTION.—The United States District Court for the District of Columbia shall have exclusive jurisdiction over any claim arising under this subsection.

(8) DEFINITIONS.—In this section:

(A) AGENCY.—The term ''agency'' has the meaning given that term in section 552(f) of title 5, United States Code.

(B) COVERED COUNTRY.—The term ''covered country'' means a country or regional economic integration organization, or member country of such organization, designated in accordance with paragraph (4).

(C) COVERED PERSON.—The term ''covered person'' means a natural person (other than an individual) who is a citizen of a covered country.

(D) COVERED RECORD.—The term ''covered record'' has the same meaning for a covered person as a record has for an individual under section 552a of title 5, United States Code, once the covered record is transferred—

(i) by a public authority of, or private entity within, a country or regional economic organization, or member country of such organization, which at the time the record is transferred is a covered country; and

(ii) to a designated Federal agency or component for purposes of preventing, investigating, detecting, or prosecuting criminal offenses.

(E) DESIGNATED FEDERAL AGENCY OR COMPONENT.—The term ''designated Federal agency or component'' means a Federal agency or component of an agency designated in accordance with paragraph (5).

(F) INDIVIDUAL.—The term ''individual'' has the meaning given that term in section 552a(a)(2) of title 5, United States Code.

(9) PRESERVATION OF PRIVILEGES.—Nothing in this subsection shall be construed to waive any applicable privilege or require the disclosure of classified information. Upon an agency's request, the district court shall review in camera and ex parte any submission by the agency in connection with this paragraph.

(10) EFFECTIVE DATE.—This section shall take effect 90 days after the date of the enactment of this Act.

SA 2590. Mr. CARDIN (for himself, Ms. MIKULSKI, Mr. WARNER, Mr. KAINE, and Ms. BALDWIN) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. RECOVER ACT.

(a) SHORT TITLE.—This section may be cited as the ''Reducing the Effects of the Cyberattack on OPM Victims Emergency Response Act of 2015'' or the ''RECOVER Act''.

(b) DEFINITION.—In this section, the term ''affected individual'' means any individual whose personally identifiable information was compromised during—

(1) the data breach of personnel records of current and former Federal employees, at a network maintained by the Department of the Interior, that was announced by the Office of Personnel Management on June 4, 2015; or

(2) the data breach of systems of the Office of Personnel Management containing information related to the background investigations of current, former, and prospective Federal employees, and of other individuals.

(c) IDENTITY PROTECTION COVERAGE FOR INDIVIDUALS AFFECTED BY FEDERAL AGENCY DATA BREACHES.—The Office of Personnel Management shall provide to each affected individual complimentary identity protection coverage that—

(1) is not less comprehensive than the complimentary identify protection coverage that the Office provided to affected individuals before the date of enactment of this Act;

(2) is effective for the remainder of the life of the individual; and

(3) includes not less than $5,000,000 in identity theft insurance.

SA 2591. Mr. SANDERS submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE II—COMMISSION ON PRIVACY RIGHTS IN THE DIGITAL AGE

SEC. 201. SHORT TITLE.

This title may be cited as the ''Commission on Privacy Rights in the Digital Age Act of 2015''.

SEC. 202. FINDINGS.

Congress makes the following findings:

(1) Today, technology that did not exist 30 years ago pervades every aspect of life in the United States.

(2) Nearly ⅔ of adults in the United States own a smartphone, and 43 percent of adults in the United States rely solely on their cell phone for telephone use.

(3) 84 percent of households in the United States own a computer and 73 percent of households in the United States have a computer with an Internet broadband connection.

(4) Federal policies on privacy protection have not kept pace with the rapid expansion of technology.

(5) Innovations in technology have led to the exponential expansion of data collection by both the public and private sectors.

(6) Consumers are often unaware of the collection of their data and how their information can be collected, bought, and sold by private companies.

SEC. 203. PURPOSE.

The purpose of this title is to establish, for a 2-year period, a Commission on Privacy Rights in the Digital Age to—

(1) examine—

(A) the ways in which public agencies and private companies gather data on the people of the United States; and

(B) the ways in which that data is utilized, either internally or externally; and

(2) make recommendations concerning potential policy changes needed to safeguard the privacy of the people of the United States.

SEC. 204. COMPOSITION OF THE COMMISSION.

(a) ESTABLISHMENT.—To carry out the purpose of this title, there is established in the legislative branch a Commission on Privacy Rights in the Digital Age (in this title referred to as the ''Commission'').

(b) COMPOSITION.—The Commission shall be composed of 13 members, as follows:

(1) Five members appointed by the President, of whom—

(A) 2 shall be appointed from the executive branch of the Government; and

(B) 3 shall be appointed from private life.

(2) Two members appointed by the majority leader of the Senate, of whom—

(A) 1 shall be a Member of the Senate; and

(B) 1 shall be appointed from private life.

(3) Two members appointed by the minority leader of the Senate, of whom—

(A) 1 shall be a Member of the Senate; and

(B) 1 shall be appointed from private life.

(4) Two members appointed by the Speaker of the House of Representatives, of whom—

(A) 1 shall be a Member of the House; and

(B) 1 shall be appointed from private life.

(5) Two members appointed by the minority leader of the House of Representatives, of whom—

(A) 1 shall be a Member of the House; and

(B) 1 shall be appointed from private life.

(c) CHAIRPERSON.—The Commission shall elect a Chairperson and Vice-Chairperson from among its members.

(d) MEETINGS; QUORUM; VACANCIES.—

(1) MEETINGS.—After its initial meeting, the Commission shall meet upon the call of the Chairperson or a majority of its members.

(2) QUORUM.—Seven members of the Commission shall constitute a quorum.

(3) VACANCIES.—Any vacancy in the Commission shall not affect its powers but shall be filled in the same manner in which the original appointment was made.

(e) APPOINTMENT OF MEMBERS; INITIAL MEETING.—

(1) APPOINTMENT OF MEMBERS.—Each member of the Commission shall be appointed not later than 60 days after the date of enactment of this Act.

(2) INITIAL MEETING.—On or after the date on which all members of the Commission have been appointed, and not later than 60 days after the date of enactment of this Act, the Commission shall hold its initial meeting.

SEC. 205. DUTIES OF THE COMMISSION.

The Commission shall—

(1) conduct an investigation of relevant facts and circumstances relating to the expansion of data collection and surveillance practices in the public, private, and national security sectors, including implications for—

(A) constitutional and statutory rights of privacy;

(B) transparency, as it relates to—

(i) government practices;

(ii) consumers; and

(iii) shareholders;

(C) waste, fraud, and abuse; and

(D) the effectiveness of congressional oversight; and

(2) submit to the President and Congress reports containing findings, conclusions, and recommendations for corrective measures relating to the facts and circumstances investigated under paragraph (1), in accordance with section 212.

SEC. 206. POWERS OF THE COMMISSION.

(a) IN GENERAL.—

(1) HEARINGS AND EVIDENCE.—The Commission or, at its direction, any subcommittee or member of the Commission, may, for the purpose of carrying out this title—

(A) hold such hearings, sit and act at such times and places, take such testimony, receive such evidence, and administer such oaths as the Commission or such subcommittee or member determines advisable; and

(B) subject to paragraph (2)(A), require, by subpoena or otherwise, the attendance and testimony of such witnesses and the production of such books, records, correspondence, memoranda, papers, documents, tapes, and materials as the Commission or such subcommittee or member determines advisable.

(2) SUBPOENAS.—

(A) ISSUANCE.—

(i) IN GENERAL.—A subpoena may be issued under paragraph (1) only—

(I) by the agreement of the Chairperson and the Vice Chairperson; or

(II) by the affirmative vote of 8 members of the Commission.

(ii) SIGNATURE.—Subject to clause (i), a subpoena issued under paragraph (1) may—

(I) be issued under the signature of—

(aa) the Chairperson; or

(bb) a member designated by a majority of the Commission; and

(II) be served by—

(aa) any person designated by the Chairperson; or

(bb) a member designated by a majority of the Commission.

(B) ENFORCEMENT.—

(i) IN GENERAL.—In the case of contumacy or failure to obey a subpoena issued under paragraph (1), the United States district court for the judicial district in which the subpoenaed person resides, is served, or may be found, or where the subpoena is returnable, may issue an order requiring such person to appear at any designated place to testify or to produce documentary or other evidence.

(ii) CONTEMPT OF COURT.—Any failure to obey the order of the court under clause (i) may be punished by the court as a contempt of that court.

(3) WITNESS ALLOWANCES AND FEES.—

(A) IN GENERAL.—Section 1821 of title 28, United States Code, shall apply to witnesses requested or subpoenaed to appear at any hearing of the Commission.

(B) SOURCE OF FUNDS.—The per diem and mileage allowances for witnesses shall be paid from funds available to pay the expenses of the Commission.

(b) CONTRACTING.—The Commission may, to such extent and in such amounts as are provided in appropriations Acts, enter into

contracts to enable the Commission to discharge its duties under this title.

(c) INFORMATION FROM FEDERAL AGENCIES.—

(1) IN GENERAL.—The Commission may secure directly from any Federal department or agency such information as the Commission considers necessary to carry out this title.

(2) FURNISHING OF INFORMATION.—If the Chairperson, the chairperson of any subcommittee created by a majority of the Commission, or any member designated by a majority of the Commission submits to a Federal department or agency a request for information under paragraph (1), the head of the department or agency shall, to the extent authorized by law, furnish the information directly to the Commission.

(3) RECEIPT, HANDLING, STORAGE, AND DISSEMINATION.—Information furnished under paragraph (2) shall only be received, handled, stored, and disseminated by members of the Commission and its staff consistent with all applicable statutes, regulations, and executive orders.

(d) ASSISTANCE FROM FEDERAL AGENCIES.—

(1) GENERAL SERVICES ADMINISTRATION.—The Administrator of General Services shall provide to the Commission on a reimbursable basis administrative support and other services for the performance of the Commission's functions.

(2) OTHER DEPARTMENTS AND AGENCIES.—In addition to the assistance provided under paragraph (1), departments and agencies of the United States may provide to the Commission such services, funds, facilities, staff, and other support services as the departments and agencies may determine advisable and as authorized by law.

(e) POSTAL SERVICES.—The Commission may use the United States mails in the same manner and under the same conditions as a department or agency of the United States.

SEC. 207. WHISTLEBLOWER PROTECTION.

(a) DISCHARGE OR DISCRIMINATION PROHIBITED.—No employer may discharge, demote, suspend, threaten, harass, or otherwise discriminate against an employee with respect to the terms and conditions of employment because the employee, or any person acting pursuant to a request of the employee—

(1) commenced, caused to be commenced, or is about to commence or cause to be commenced a proceeding with the Commission under this title;

(2) testified or is preparing to testify in a proceeding described in paragraph (1);

(3) lawfully assisted or is preparing to lawfully assist in any manner in a proceeding described in paragraph (1) or in any other action to carry out the purposes of this title; or

(4) refuses to violate the provisions of this title.

(b) ENFORCEMENT ACTION.—

(1) IN GENERAL.—An employee who alleges discharge or other discrimination by an employer in violation of subsection (a) may seek relief under subsection (c) by—

(A) filing a complaint with the Secretary of Labor; or

(B) if the Secretary of Labor has not issued a final decision within 180 days of the filing of the complaint and there is no showing that such delay is due to the bad faith of the claimant, bringing an action at law or equity for de novo review in the appropriate district court of the United States, which shall have jurisdiction over such an action without regard to the amount in controversy.

(2) PROCEDURE.—

(A) IN GENERAL.—A complaint filed under paragraph (1)(A) shall be governed under the rules and procedures set forth in section 42121(b) of title 49, United States Code.

(B) EXCEPTION.—Notification made under section 42121(b)(1) of title 49, United States Code, shall be made to any individual named in the complaint and to the employer.

(C) BURDENS OF PROOF.—An action brought under paragraph (1)(B) shall be governed by the legal burdens of proof set forth in section 42121(b) of title 49, United States Code.

(D) STATUTE OF LIMITATIONS.—A complaint under paragraph (1)(A) shall be filed not later than 180 days after the date on which the violation occurs, or after the date on which the employee became aware of the violation.

(E) JURY TRIAL.—A party to an action brought under paragraph (1)(B) shall be entitled to trial by jury.

(c) REMEDIES.—

(1) IN GENERAL.—An employee prevailing in any action under subsection (b)(1) shall be entitled to all relief necessary to make the employee whole.

(2) COMPENSATORY DAMAGES.—Relief for any action under paragraph (1) shall include—

(A) reinstatement with the same seniority status that the employee would have had, but for the discrimination;

(B) the amount of back pay, with interest; and

(C) compensation for any special damages sustained as a result of the discrimination, including litigation costs, expert witness fees, and reasonable attorney fees.

(d) RIGHTS RETAINED BY EMPLOYEE.—Nothing in this section shall be deemed to diminish the rights, privileges, or remedies of any employee under any Federal or State law, or under any collective bargaining agreement.

(e) NONENFORCEABILITY OF CERTAIN PROVISIONS WAIVING RIGHTS AND REMEDIES OR REQUIRING ARBITRATION OF DISPUTES.—

(1) WAIVER OF RIGHTS AND REMEDIES.—The rights and remedies provided for in this section may not be waived by any agreement, policy form, or condition of employment, including by a predispute arbitration agreement.

(2) PREDISPUTE ARBITRATION AGREEMENTS.—No predispute arbitration agreement shall be valid or enforceable, if the agreement requires arbitration of a dispute arising under this section.

SEC. 208. NONAPPLICABILITY OF FEDERAL ADVISORY COMMITTEE ACT.

(a) IN GENERAL.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Commission.

(b) PUBLIC HEARINGS AND MEETINGS.—The Commission shall—

(1) hold public hearings and meetings to the extent appropriate; and

(2) conduct public hearings and meetings in a manner consistent with the protection of information provided to or developed for or by the Commission as required by any applicable statute, regulation, or executive order.

SEC. 209. STAFF OF COMMISSION.

(a) IN GENERAL.—

(1) APPOINTMENT AND COMPENSATION.—The Chairperson, in consultation with the Vice Chairperson and in accordance with rules agreed upon by the Commission, may appoint and fix the compensation of an executive director and such other personnel as may be necessary to enable the Commission to carry out the functions of the Commission, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to the provisions of chapter 51 and subchapter III of chapter 53 of that title relating to classification and General Schedule pay rates, except that no rate of pay fixed under this paragraph may exceed the equivalent of that payable for a position at level V of the Executive Schedule under section 5316 of title 5, United States Code.

(2) PERSONNEL AS FEDERAL EMPLOYEES.—

(A) IN GENERAL.—The executive director and any personnel of the Commission who are employees shall be employees under section 2105 of title 5, United States Code, for purposes of chapters 63, 81, 83, 84, 85, 87, 89, 89A, 89B, and 90 of that title.

(B) MEMBERS OF COMMISSION.—Subparagraph (A) shall not be construed to apply to members of the Commission.

(b) DETAILEES.—Any Federal Government employee may be detailed to the Commission without reimbursement from the Commission, and such detailee shall retain the rights, status, and privileges of his or her regular employment without interruption.

(c) CONSULTANT SERVICES.—The Commission may procure the services of experts and consultants in accordance with section 3109 of title 5, United States Code, but at rates not to exceed the daily rate paid a person occupying a position at level IV of the Executive Schedule under section 5315 of that title.

SEC. 210. COMPENSATION AND TRAVEL EXPENSES.

(a) COMPENSATION.—Each member of the Commission who is not an officer or employee of the Federal Government may be compensated at not to exceed the daily equivalent of the annual rate of basic pay in effect for a position at level IV of the Executive Schedule under section 5315 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Commission.

(b) TRAVEL EXPENSES.—While away from their homes or regular places of business in the performance of services for the Commission, members of the Commission shall be allowed travel expenses, including per diem in lieu of subsistence, in the same manner as persons employed intermittently in the Government service are allowed expenses under section 5703 of title 5, United States Code.

SEC. 211. SECURITY CLEARANCES FOR COMMISSION MEMBERS AND STAFF.

The appropriate departments or agencies of the Federal Government shall cooperate with the Commission in expeditiously providing to the members and staff of the Commission appropriate security clearances, up to the level of sensitive compartmented information, to the extent possible under applicable procedures and requirements, and no person shall be provided with access to classified information under this title without the appropriate security clearances.

SEC. 212. REPORTS OF COMMISSION; TERMINATION.

(a) INTERIM REPORTS.—The Commission shall submit to the President and Congress, and make publicly available online, interim reports containing such findings, conclusions, and recommendations for corrective measures as have been agreed to by a majority of Commission members.

(b) FINAL REPORT.—Not later than 2 years after the date of enactment of this Act, the Commission shall submit to the President and Congress, and make publicly available online, a final report containing such findings, conclusions, and recommendations for corrective measures as have been agreed to by a majority of Commission members.

(c) CLASSIFIED INFORMATION.—Each report submitted under subsection (a) or (b) shall be in unclassified form, but may include a classified annex.

(d) TERMINATION.—

(1) IN GENERAL.—The Commission, and all the authorities under this title, shall terminate 60 days after the date on which Commission submits the final report under subsection (b).

(2) ADMINISTRATIVE ACTIVITIES BEFORE TERMINATION.—The Commission may use the 60-

day period referred to in paragraph (1) for the purpose of concluding its activities, including providing testimony to committees of Congress concerning its reports and disseminating the final report.

SEC. 213. FUNDING.

(a) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as are necessary to carry out this title.

(b) DURATION OF AVAILABILITY.—Amounts made available to the Commission under subsection (a) shall remain available until the termination of the Commission.

SA 2592. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. WHISTLEBLOWER REPORTS AND PROTECTION AGAINST RETALIATION.

(a) AUTHORIZATION TO REPORT COMPLAINTS OR INFORMATION.—An employee of or contractor to a Federal entity that has knowledge of the programs and activities authorized under this Act may submit a covered complaint—

(1) to the Comptroller General of the United States;

(2) to the Privacy and Civil Liberties Oversight Board;

(3) to the Select Committee on Intelligence of the Senate;

(4) to the Permanent Select Committee on Intelligence of the House of Representatives; or

(5) in accordance with the process established under section 103H(k)(5) of the National Security Act of 1947 (50 U.S.C. 3033(k)(5)).

(b) INVESTIGATIONS AND REPORTS TO CONGRESS.—

(1) IN GENERAL.—The Comptroller General shall investigate a covered complaint submitted pursuant to subsection (a)(1) and shall submit to Congress a report containing the results of the investigation.

(2) AVAILABILITY TO CONGRESS.—A report submitted to Congress under paragraph (1) shall be accessible to all members of Congress.

(c) REQUIREMENT TO PERMIT SUBMISSION.—No Federal entity may promulgate a rule or prohibition on its employees, on contractors of that Federal entity, or on any entity sharing cyber threat indicators or defensive measures with the Federal Government under this Act that prohibits submission of complaints under this section.

(d) PROHIBITION ON RETALIATORY ACTIONS.—Notwithstanding any other provision of law, no officer or employee of a Federal entity shall take any retaliatory action against an employee of or contractor to a Federal entity who seeks to disclose or discloses covered information to—

(1) the Comptroller General;

(2) the Privacy and Civil Liberties Oversight Board;

(3) the Select Committee on Intelligence of the Senate;

(4) the Permanent Select Committee on Intelligence of the House of Representatives; or

(5) the Office of the Inspector General of the Intelligence Community.

(e) ADMINISTRATIVE SANCTIONS.—An officer or employee of a Federal entity who violates subsection (d) shall be subject to administrative sanctions, up to and including termination.

(f) DEFINITIONS.—In this section:

(1) COVERED COMPLAINT.—The term ''covered complaint'' means a complaint or information concerning programs and activities authorized by this Act that an employee or contractor reasonably believes is evidence of—

(A) a violation of any law, rule, or regulation; or

(B) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

(2) COVERED INFORMATION.—The term ''covered information'' means any information (including classified or sensitive information) that an employee or contractor reasonably believes is evidence of—

(A) a violation of any provision of law; or

(B) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

SA 2593. Mr. DURBIN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 18, line 24, strike ''records.'' and insert ''records, except disclosure required under any State, tribal, or local law in any criminal prosecution.''.

On page 32, line 17, strike ''Cyber'' and insert ''Except for disclosure of evidence required by law or rule in any criminal prosecution, cyber''.

SA 2594. Mr. DURBIN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 48, between lines 8 and 9, insert the following:

(3) CONSTRUCTION REGARDING OPERATION OF DEFENSIVE MEASURES AND TORT LIABILITY.—Nothing in this Act shall be construed to supersede any statute or other provision of law of a State or political subdivision of a State that establishes a right of action or remedy for damages to a party other than an entity described in section 4(b)(1) resulting from the operation of a defensive measure under this Act.

SA 2595. Mr. DURBIN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 35, line 6, strike ''Cyber'' and insert

(i) IN GENERAL.—Cyber

On page 35, between lines 11 and 12, insert the following:

(ii) LIMITATION ON USE IN PROCEEDINGS.—Cyber threat indicators, defensive measures, and any other information provided to the Federal Government under this Act and all evidence derived therefrom may not be received in evidence in any trial, hearing or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or any political subdivision thereof if the sharing, disclosure or use of such cyber threat indicator, defensive measure, or other information was or would be in violation of this Act.

SA 2596. Mr. DURBIN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 11, line 10, strike ''contravention;'' and insert ''contravention, and instructions to remedy or mitigate such error or contravention, including the destruction of such cyber threat indicator and the cessation of any defensive measures based on such indicator;''.

On page 15, between lines 16 and 17, insert the following:

(3) NOTIFICATION AND MITIGATION OF ERROR OR CONTRAVENTION.—

(A) REQUIREMENT TO NOTIFY.—An entity that shares a cyber threat indicator or defensive measure and subsequently determines that such cyber threat indicator or defensive measure was in error or in contravention of the requirements of this Act or another provision of Federal law or policy shall notify each entity with which such indicator or measure was shared of such error or contravention.

(B) REQUIREMENTS FOR RECEIVING ENTITY.—An entity that receives a notice under subparagraph (A)—

(i) shall cease use of such cyber threat indicator or defensive measure;

(ii) shall not further share such indicator or measure; and

(iii) shall provide a similar notice to each other entity with which the receiving entity has shared such indicator or measure.

On page 17, between lines 16 and 17, insert the following:

(II) a notification of error or contravention received from a Federal entity or sharing entity pursuant to section 3(b)(1)(C) or section 4(c)(3); or

---

SA 2597. Mrs. SHAHEEN submitted an amendment intended to be proposed by her to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 10, line 8, strike ''and''.

On page 10, line 13, strike the period at the end and insert ''; and''.

On page 10, between lines 13 and 14, insert the following:

(5) the periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analysis of cyber threat indicators and information in possession of the Federal Government, with attention to accessibility and implementation challenges faced by small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 632)).

On page 12, line 13, insert ''the Small Business Administration and'' after ''including''.

SA 2598. Mr. FRANKEN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other

purposes; which was ordered to lie on the table; as follows:

Beginning on page 5, strike line 10 and all that follows through page 52, line 6, and insert the following:

(7) 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).

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

(9) 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.

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

(11) 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.

(12) 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.

(13) 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.

(14) 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).

(15) 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.

(16) 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.

(17) 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. 3. 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 Act that is known or determined to be in error or in contravention of the requirements of this Act or another provision of Federal law or policy of such error or contravention;

(D) include requirements for Federal entities receiving cyber threat indicators to implement and utilize security controls to protect against unauthorized access to or acquisition of such cyber threat indicators; 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 2 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 Act, 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. 4. 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 Act; or

(B) to limit otherwise lawful activity.

(b) AUTHORIZATION FOR SHARING OR RECEIVING CYBER THREAT INDICATORS.—

(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 Act and consistent with the protection of classified information, share with, or receive from, any other entity or the Federal Government a cyber threat indicator.

(2) LAWFUL RESTRICTION.—An entity receiving a cyber threat indicator from another entity or Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator 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 other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

(c) PROTECTION AND USE OF INFORMATION.—

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

(2) REMOVAL OF CERTAIN PERSONAL INFORMATION.—An entity sharing a cyber threat indicator pursuant to this Act 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 BY ENTITIES.—

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

(i) be used by an entity to monitor—

(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

(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 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 5(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 shared with a State, tribal, or local government under this Act 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 or sharing of a cyber threat indicator.

(ii) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—A cyber threat indicator 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.

(d) ANTITRUST EXEMPTION.—

(1) IN GENERAL.—Except as provided in section 8(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 Act.

(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.

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

SEC. 5. SHARING OF CYBER THREAT INDICATORS 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 Act, 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 by the Federal Government.

(2) FINAL POLICIES AND PROCEDURES.—Not later than 180 days after the date of the enactment of this Act, 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 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 4(b) 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 4 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 Act, 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 Act, 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 Act 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 Act, 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 Act.

(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 Act 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 Act.

(b) PRIVACY AND CIVIL LIBERTIES.—

(1) GUIDELINES OF ATTORNEY GENERAL.—Not later than 60 days after the date of the enactment of this Act, 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 Act.

(2) FINAL GUIDELINES.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, 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 Act.

(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 Act;

(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 Act; 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 Act; 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 Act, 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, 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 under this Act 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 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 under this Act; 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 through such process with the Federal Government; and

(B) all of the appropriate Federal entities receive such cyber threat indicators 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 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 Act, 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 to the Federal Government under this Act shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

(2) PROPRIETARY INFORMATION.—Consistent with section 4(b)(2), a cyber threat indicator provided by an entity to the Federal Government under this Act 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 provided to the Federal Government under this Act 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 to the Federal Government under this Act shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

(5) DISCLOSURE, RETENTION, AND USE.—

(A) AUTHORIZED ACTIVITIES.—Cyber threat indicators provided to the Federal Government under this Act 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 provided to the Federal Government under this Act 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 provided to the Federal Government under this Act 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 provided to the Federal Government under this Act 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 or sharing cyber threat indicators.

(ii) EXCEPTIONS.—

(I) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—Cyber threat indicators provided to the Federal Government under this Act 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 ACT.—Clause (i) shall not apply to procedures developed and implemented under this Act.

SEC. 6. 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 4(a) that is conducted in accordance with this Act.

(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 under section 4(b) if—

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

(2) in a case in which a cyber threat indicator is shared with the Federal Government, the cyber threat indicator is shared in a manner that is consistent with section

5(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 5(a)(1); or

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

(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 Act; or

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

SEC. 7. 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 Act, 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 Act.

(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 5 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 5(c), including any impediments to such real-time sharing.

(C) An assessment of the sufficiency of the procedures developed under section 3 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 Act.

(E) A review of the type of cyber threat indicators shared with the Federal Government under this Act, 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 Act, including the appropriateness of any subsequent use or dissemination of such cyber threat indicators by a Federal entity under section 5.

(G) A description of any significant violations of the requirements of this Act 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 Act 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 Act.

(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 Act 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 Act; and

(B) an assessment of the sufficiency of the policies, procedures, and guidelines established pursuant to section 5 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 Act 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 that have been shared with Federal entities under this Act.

(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 Act.

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

SEC. 8. CONSTRUCTION AND PREEMPTION.

(a) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this Act 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 Act; 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 Act.

(b) WHISTLE BLOWER PROTECTIONS.—Nothing in this Act 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 Act 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 Act 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 Act 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 Act 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 5(c).

(g) PRESERVATION OF CONTRACTUAL OBLIGATIONS AND RIGHTS.—Nothing in this Act 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 Act 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 Act shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized in this Act.

(j) USE AND RETENTION OF INFORMATION.—Nothing in this Act 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 Act for any use other than permitted in this Act.

(k) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This Act 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 Act.

(2) STATE LAW ENFORCEMENT.—Nothing in this Act 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 Act shall be construed—

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

(2) to establish or limit any regulatory authority not specifically established or limited under this Act; 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 Act 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. 9. REPORT ON CYBERSECURITY THREATS.

(a) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, 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. 10. 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 such information is shared consistent with the policies and procedures promulgated by the Attorney General under section 5 of the Cybersecurity Information Sharing Act of 2015.''.

SA 2599. Mr. FRANKEN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 14, line 5, strike ''provision of law,'' and insert ''statute or regulation,''.

SA 2600. Mr. FRANKEN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 13, line 6, strike ''provision of law,'' and insert ''statute or regulation,''.

SA 2601. Mr. FRANKEN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 15, strike lines 4 through 10 and insert the following:

(1) IN GENERAL.—Except as provided in paragraph (2) and notwithstanding any other statute or regulation, an entity may, for a cybersecurity purpose, and in accordance with the provisions of this Act 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.

SA 2602. Mr. FRANKEN submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 3, line 21, strike ''may'' and insert ''is reasonably likely to''.

SA 2603. Mr. KIRK (for himself and Mrs. GILLIBRAND) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ____. APPREHENSION AND PROSECUTION OF INTERNATIONAL CYBER CRIMINALS.

(a) INTERNATIONAL CYBER CRIMINAL DEFINED.—In this section, the term ''international cyber criminal'' means an individual—

(1) who is physically present within a country with which the United States does not have a mutual legal assistance treaty or an extradition treaty;

(2) who is believed to have committed a cybercrime or intellectual property crime against the interests of the United States or its citizens; and

(3) for whom—

(A) an arrest warrant has been issued by a judge in the United States; or

(B) an international wanted notice (commonly referred to as a ''Red Notice'') has been circulated by Interpol.

(b) BILATERAL CONSULTATIONS.—The Secretary of State, or designee, shall consult with the appropriate government official of each country in which one or more international cyber criminals are physically present to determine what actions the government of such country has taken—

(1) to apprehend and prosecute such criminals; and

(2) to prevent such criminals from carrying out cybercrimes or intellectual property crimes against the interests of the United States or its citizens.

(c) ANNUAL REPORT.—

(1) IN GENERAL.—The Secretary of State shall submit to the appropriate congressional committees an annual report that identifies—

(A) the number of international cyber criminals who are located in countries that do not have an extradition treaty or mutual legal assistance treaty with the United States, broken down by country;

(B) the dates on which an official of the Department of State, as a result of this Act, discussed ways to thwart or prosecute international cyber criminals in a bilateral conversation with an official of another country, including the name of each such country; and

(C) for each international cyber criminal who was extradited into the United States during the most recently completed calendar year—

(i) his or her name;

(ii) the crimes for which he or she was charged;

(iii) his or her previous country of residence; and

(iv) the country from which he or she was extradited into the United States.

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—For purposes of this subsection, the term ''appropriate congressional committees'' means—

(A) the Committee on Foreign Relations of the Senate;

(B) the Committee on Appropriations of the Senate;

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

(D) the Committee on Banking, Housing, and Urban Affairs of the Senate;

(E) the Committee on Foreign Affairs of the House of Representatives;

(F) the Committee on Appropriations of the House of Representatives;

(G) the Committee on Homeland Security of the House of Representatives; and

(H) the Committee on Financial Services of the House of Representatives.

SA 2604. Mr. COATS submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 51, strike line 8 and insert the following:

SEC. 10. STUDY ON CYBERSECURITY THREATS TO MOBILE DEVICES.

(a) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Secretary of Homeland Security shall—

(1) complete a study on cybersecurity threats relating to mobile devices; and

(2) submit a report to Congress that contains the findings of such study and the recommendations developed under subsection (b)(3).

(b) MATTERS STUDIED.—In carrying out the study under subsection (a)(1), the Secretary shall—

(1) assess cybersecurity threats relating to mobile devices;

(2) assess the effect such threats may have on the cyber security of the information systems and networks of the Federal Government (except for the information systems and networks of the Department of Defense and the Intelligence Community); and

(3) develop recommendations for addressing such threats.

SEC. 11. CONFORMING AMENDMENTS.

SA 2605. Ms. WARREN submitted an amendment intended to be proposed by her to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. STRENGTHENING PUBLIC NOTIFICATION REQUIREMENTS.

Section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) is amended—

(1) by redesignating paragraphs (1) through (3) as subparagraphs (A) through (C), respectively, and adjusting the margins accordingly;

(2) in the matter preceding subparagraph (A), as so redesignated, by striking ''In furtherance'' and inserting the following:

''(1) IN GENERAL.—In furtherance''; and

(3) by adding at the end the following:

''(2) STANDARDS NOT LIMITED TO UNAUTHORIZED ACCESS OR USE OF SENSITIVE CUSTOMER RECORD OR INFORMATION.—The standards established in accordance with paragraph (1)—

''(A) shall require financial institutions to disclose the unauthorized access to or use of any customer record or information; and

''(B) shall not be limited to only require financial institutions to disclose the unauthorized access to or use of sensitive customer records or information.''.

SA 2606. Ms. WARREN submitted an amendment intended to be proposed by her to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. IMPROVING EXPERTISE OF BANKING REGULATORS.

(a) DEFINITIONS.—In this section—

(1) the term ''appropriate Federal banking agency'' has the meaning given that term in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813);

(2) the term ''banking regulators'' means—

(A) the appropriate Federal banking agencies; and

(B) the National Credit Union Administration; and

(3) the term ''covered entity'' means any entity that—

(A) is subject to examination by a banking regulator;

(B) has more than $10,000,000,000 in assets.

(b) PARTICIPATION IN EXAMINATION OF COVERED ENTITIES BY SPECIALISTS.—Each banking regulator shall ensure that an information security specialist participates in an examination by the banking regulator of a covered entity not less frequently than once every 3 years.

(c) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to alter the frequency of examinations conducted by a banking regulator.

SA 2607. Ms. WARREN submitted an amendment intended to be proposed by her to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. REGULATION AND EXAMINATION OF SERVICE PROVIDERS.

Title II of the Federal Credit Union Act (12 U.S.C. 1781 et seq.) is amended by striking section 206A (12 U.S.C. 1786a) and inserting the following:

''SEC. 206A. REGULATION AND EXAMINATION OF SERVICE PROVIDERS.

''(a) SERVICE PERFORMED BY CONTRACT OR OTHERWISE.—If an insured credit union that is regularly examined or subject to examination by the Board, causes to be performed for itself, by contract or otherwise, any service authorized under this Act, or in the case of a State credit union, any applicable State law, whether on or off its premises—

''(1) such performance, including any cybersecurity practice, shall be subject to regulation and examination by the Board to the same extent as if such services were being performed by the insured credit union itself on its own premises; and

''(2) the insured credit union shall notify the Board of the existence of the service relationship not later than 30 days after the earlier of—

''(A) the date on which the contract is entered into; or

''(B) the date on which the performance of the service is initiated.

''(b) ADMINISTRATION BY THE BOARD.—The Board may issue such regulations and orders as may be necessary to enable the Board to administer and carry out this section and to prevent evasion of this section.''.

SA 2608. Ms. WARREN submitted an amendment intended to be proposed by her to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 39, between lines 12 and 13, insert the following:

(3) to protect an entity from liability for a failure to take action to address a cybersecurity threat or a security vulnerability.

SA 2609. Ms. WARREN submitted an amendment intended to be proposed by her to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

In section 6, after subsection (b), insert the following:

(c) LIABILITY FOR FAILURE TO ACT.—An entity that receives information regarding a cybersecurity threat or a security vulnerability under this Act shall take action to address the threat or vulnerability or the entity may be subject to liability for a failure to act.

SA 2610. Ms. KLOBUCHAR submitted an amendment intended to be proposed by her to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. DHS ANNUAL REPORT ON ECONOMIC IMPLICATIONS OF CYBER ATTACKS.

(a) ANNUAL REPORT.—Not later than 1 year after the date of enactment of this Act, and once every year thereafter, the Secretary of Homeland Security shall submit to Congress a report detailing the economic impact of cyber attacks during the year for which the report is prepared and the year-to-year trends of the economic impact of cyber attacks, in aggregate form, including—

(1) an estimate of losses (in dollars) as a result of cyber attacks; and

(2) the approximate number of cyber attacks on the networks of private entities that have been reported to the Department of Homeland Security.

(b) PROHIBITION.—Each report submitted under subsection (a) may not include the name, or other identifying information, of any private entity that has experienced a cyber attack.

SA 2611. Ms. KLOBUCHAR submitted an amendment intended to be proposed by her to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. GAO REPORT ON IMPLEMENTATION.

(a) STUDY.—The Comptroller General of the United States shall conduct a study on the implementation of the information sharing system developed under this Act.

(b) REPORT.—Not later than 1 year after the date on which the information sharing procedures described in this Act are implemented, the Comptroller General shall submit to Congress a report on the study conducted under subsection (a), which shall include an assessment of—

(1) the effectiveness of the information sharing system in sharing cyber threat indicators, including an approximate number of cyber threat indicators shared;

(2) the extent to which the information sharing procedures described in this Act—

(A) are used by private entities; and

(B) are effective at screening out personal information or information that identifies a specific person not directly related to a cybersecurity threat;

(3) the extent to which private entities have implemented procedures to remove personal information or information that identifies a specific person not directly related to a cybersecurity threat prior to sharing cyber threat indicators with a Federal entity, consistent with the requirements of this Act;

(4) the extent to which the Department of Homeland Security has implemented procedures to remove personal information or information that identifies a specific person not directly related to a cybersecurity threat prior to sharing cyber threat indicators with private entities or other Federal entities, consistent with the requirements of this Act; and

(5) the effectiveness of data security implemented by Federal entities that are involved in the sharing of cyber threat indicators.

SA 2612. Mr. FRANKEN (for himself, Mr. LEAHY, and Mr. WYDEN) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

Beginning on page 3, strike line 21 and all that follows through page 5, line 8, and insert the following:

system that is reasonably likely to 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 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 information is not otherwise prohibited by law; or

---

SA 2613. Mr. CARPER submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 22, strike lines 13 through 19 and insert the following:

(i) are shared in as close to real time as practicable with all appropriate Federal entities and in accordance with Attorney General policies, procedures, and guidelines and any applicable statutory requirements; and

On page 22, line 20, strike ''(iii)'' and insert ''(ii)''.

On page 30, strike lines 4 through 8 and insert the following:

(C) ensures that the appropriate Federal entities receive such cyber threat indicators in as close to real time as practicable and in accordance with Attorney General policies, procedures, and guidelines and any applicable statutory requirements;

Beginning on page 31, strike line 20 and all that follows through page 32, line 6, and insert the following:

(B) the appropriate Federal entities receive such cyber threat indicators and defensive measures through the process within the Department of Homeland Security in as close to real time as practicable and in accordance with Attorney General policies, procedures, and guidelines and any applicable statutory requirements.

(4) OTHER FEDERAL ENTITIES.—The process developed and implemented under paragraph (1) shall ensure that other Federal entities receive such cyber threat indicators and defensive measures shared with the Federal Government through the process in as close to real time as practicable and in accordance with Attorney General policies, procedures, and guidelines and any applicable statutory requirements.

SA 2614. Mr. CARPER submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

Strike paragraph (1) of section 4(c) and insert the following:

(1) IN GENERAL.—

(A) SHARING WITH ALL ENTITIES.—Except as provided in paragraph (2) and notwithstanding any other provision of law, an entity may, for the purposes permitted under this Act and consistent with the protection of classified information, share with, or receive from, any other entity or the Federal Government in a manner consistent with section 5(c)(1)(B) a cyber threat indicator or defensive measure.

(B) SHARING WITH FEDERAL ENTITIES.—Except as provided in paragraph (2) and consistent with other applicable laws, an entity may, for the purposes permitted under this Act and consistent with the protection of classified information, share with, or receive from, the Federal Government a cyber threat indicator or defensive measure.

SA 2615. Mr. CARPER submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

On page 22, line 16, insert ''unnecessary'' after ''delay,''.

NOTICE OF INTENT TO OBJECT TO PROCEEDING

I, Senator CHARLES E. GRASSLEY, intend to object to proceeding to the nomination of David Malcolm Robinson to be Assistant Secretary of State (Conflict and Stabilization Operations), PN337; and Coordinator for Reconstruction and Stabilization, PN336, dated August 4, 2015.

AUTHORITY FOR COMMITTEES TO MEET

COMMITTEE ON ARMED FORCES

Mr. BURR. Mr. President, I ask unanimous consent that the Committee on Armed Services be authorized to meet during the session of the Senate on August 4, 2015, at 9:30 a.m.

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

COMMITTTEE ON FINANCE

Mr. BURR. Mr. President, I ask unanimous consent that the Committee on Finance be authorized to meet during the session of the Senate on August 4, 2015, at 10 a.m., in room SD–215 of the Dirksen Senate Office Building, to conduct a hearing entitled ''A Way Back Home: Preserving Families and Reducing the Need for Foster Care.''

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

COMMITTEE ON FOREIGN RELATIONS

Mr. BURR. Mr. President, I ask unanimous consent that the Committee on Foreign Relations be authorized to meet during the session of the Senate on August 4, 2015, at 10 a.m., to conduct a hearing entitled ''JCPOA: Non-Proliferations, Inspections, and Nuclear Constraints.''

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

COMMITTEE ON FOREIGN RELATIONS

Mr. BURR. Mr. President, I ask unanimous consent that the Committee on Foreign Relations be authorized to meet during the session of the Senate on August 4, 2015, at 2:30 p.m., to conduct a hearing entitled ''Nominations.''

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

Mr. BURR. Mr. President, I ask unanimous consent that the Committee on Homeland Security and Governmental Affairs be authorized to meet during the session of the Senate on August 4,

2015, at 10 a.m., to conduct a hearing entitled ''Oversight of the Bureau of Prisons: First-Hand Accounts of Challenges Facing the Federal Prison System.''

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

SELECT COMMITTEE ON INTELLIGENCE

Mr. BURR. Mr. President, I ask unanimous consent that the Select Committee on Intelligence be authorized to meet during the session of the Senate on August 4, 2015, at 3 p.m.

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

SUBCOMMITTEE ON SUPERFUND, WASTE MANAGEMENT, AND REGULATORY OVERSIGHT

Mr. BURR. Mr. President, I ask unanimous consent that the Subcommittee on Superfund, Waste Management, and Regulatory Oversight of the Committee on Environment and Public Works be authorized to meet during the session of the Senate on August 4, 2015, at 9:30 a.m., in room SD–406 of the Dirksen Senate Office Building, to conduct a hearing entitled ''Oversight of Litigation at EPA and FWS: Impacts on the U.S. Economy, States, Local Communities and the Environment.''

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

U.S. COMMERCIAL SPACE LAUNCH COMPETITIVENESS ACT

Mr. ROUNDS. Mr. President, I ask unanimous consent that the Senate proceed to the immediate consideration of Calendar No. 159, S. 1297.

The PRESIDING OFFICER. The clerk will report the bill by title.

The senior assistant legislative clerk read as follows:

A bill (S. 1297) to update the Commercial Space Launch Act by amending title 51, United States Code, to promote competitiveness of the U.S. commercial space sector, and for other purposes.

There being no objection, the Senate proceeded to consider the bill, which had been reported from the Committee on Commerce, Science, and Transportation, with an amendment to strike all after the enacting clause and insert in lieu thereof the following:

S. 1297

SECTION 1. SHORT TITLE.

This Act may be cited as the ''U.S. Commercial Space Launch Competitiveness Act''.

SEC. 2. REFERENCES TO TITLE 51, UNITED STATES CODE.

Except as otherwise expressly provided, wherever in this Act an amendment or repeal is expressed in terms of an amendment to, or repeal of, a section or other provision, the reference shall be considered to be made to a section or other provision of title 51, United States Code.

SEC. 3. LIABILITY INSURANCE AND FINANCIAL RESPONSIBILITY REQUIREMENTS.

(a) SENSE OF CONGRESS.—It is the sense of Congress that it is in the public interest to update the methodology used to calculate the maximum probable loss from claims under section 50914 of title 51, United States Code, with a validated risk profile approach in order to consistently compute valid and reasonable maximum probable loss values.

(b) IMPLEMENTATION.—Not later than September 30, 2015, the Secretary of Transportation, in consultation with the commercial space sector and insurance providers, shall—

(1) evaluate and, if necessary, develop a plan to update the methodology used to calculate the maximum probable loss from claims under section 50914 of title 51, United States Code;

(2) in evaluating or developing a plan under paragraph (1)—

(A) ensure that the Federal Government is not exposed to greater costs than intended and that launch companies are not required to purchase more insurance coverage than necessary; and

(B) consider the impact of the cost to both the industry and the Government of implementing an updated methodology; and

(3) submit the evaluation, and any plan, to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives.

SEC. 4. LAUNCH LIABILITY EXTENSION.

Section 50915(f) is amended by striking ''December 31, 2016'' and inserting ''December 31, 2020''.

SEC. 5. COMMERCIAL SPACE LAUNCH LICENSING AND EXPERIMENTAL PERMITS.

Section 50906 is amended—

(1) in subsection (d), by striking ''launched or reentered'' and inserting ''launched or reentered under that permit'';

(2) by amending subsection (d)(1) to read as follows:

''(1) research and development to test design concepts, equipment, or operating techniques;'';

(3) in subsection (d)(3) by striking ''prior to obtaining a license'';

(4) in subsection (e)(1) by striking ''suborbital rocket design'' and inserting ''suborbital rocket or suborbital rocket design''; and

(5) by amending subsection (g) to read as follows:

''(g) The Secretary may issue a permit under this section notwithstanding any license issued under this chapter. The issuance of a license under this chapter may not invalidate a permit issued under this section.''.

SEC. 6. LICENSING REPORT.

Not later than 120 days after the date of enactment of this Act, the Secretary of Transportation shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives a report on approaches for streamlining the licensing and permitting process of launch vehicles, reentry vehicles, or components of launch or reentry vehicles, to enable non-launch flight operations related to space transportation. The report shall include approaches to improve efficiency, reduce unnecessary costs, resolve inconsistencies, remove duplication, and minimize unwarranted constraints. The report shall also include an assessment of existing private and government infrastructure, as appropriate, in future licensing activities.

SEC. 7. SPACE AUTHORITY.

(a) IN GENERAL.—Not later than 120 days after the date of enactment of this Act, the Director of the Office of Science and Technology Policy, in consultation with the Secretary of State, the Secretary of Transportation, the Administrator of the National Aeronautics and Space Administration, the heads of other relevant Federal agencies, and the commercial space sector, shall—

(1) assess current, and proposed near-term, commercial non-governmental activities conducted in space;

(2) identify appropriate oversight authorities for the activities described in paragraph (1);

(3) recommend an oversight approach that would prioritize safety, utilize existing authorities, minimize burdens, promote the U.S. commercial space sector, and meet the United States obligations under international treaties; and

(4) submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives a report on the assessment and recommended approaches.

(b) EXCEPTION.—Nothing in this section shall apply to the activities of the ISS national laboratory as described in section 504 of the National Aeronautics and Space Administration Authorization Act of 2010 (42 U.S.C. 18354), including any research or development projects utilizing the ISS national laboratory.

SEC. 8. SPACE SURVEILLANCE AND SITUATIONAL AWARENESS DATA.

Not later than 120 days after the date of enactment of this Act, the Secretary of Transportation in concurrence with the Secretary of Defense shall—

(1) in consultation with the heads of other relevant Federal agencies, study the feasibility of processing and releasing safety-related space situational awareness data and information to any entity consistent with national security interests and public safety obligations of the United States; and

(2) submit a report on the feasibility study to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives.

SEC. 9. EXTENSION OF CERTAIN SAFETY REGULATION REQUIREMENTS.

(a) EXTENSION OF CERTAIN SAFETY REGULATION REQUIREMENTS.—Section 50905(c)(3) is amended by striking ''Beginning on October 1, 2015'' and inserting ''Beginning on October 1, 2020''.

(b) CONSTRUCTION.—Section 50905(c) is amended by adding at the end the following:

''(5) Nothing in this subsection shall be construed to limit the authority of the Secretary to discuss potential regulatory approaches with the commercial space sector, including observations, findings, and recommendations from the Commercial Space Transportation Advisory Committee, prior to the issuance of a notice of proposed rulemaking.''.

(c) REPORT.—Not later than 270 days after the date of enactment of this Act, the Secretary of Transportation, in consultation with the commercial space sector, including the Commercial Space Transportation Advisory Committee, shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives a report specifying key industry metrics that might indicate readiness of the commercial space sector and the Department of Transportation to transition to a regulatory approach under section 50905(c)(3) of title 51, United States Code, that considers space flight participant, government astronaut, and crew safety.

(d) BIENNIAL REPORT.—Beginning on December 31, 2016, and biennially thereafter, the Secretary of Transportation, in consultation and coordination with the commercial space sector, including the Commercial Space Transportation Advisory Committee, shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives a report that identifies the activities, described in subsections (c) and (d) of section 50905 of title 51, United States Code, most appropriate for regulatory action, if any, and a proposed transition plan for such regulations.

SEC. 10. INDUSTRY VOLUNTARY CONSENSUS STANDARDS.

(a) INDUSTRY VOLUNTARY CONSENSUS STANDARDS.—Section 50905(c), as amended in section 9 of this Act, is further amended by adding at the end the following:

''(6) The Secretary shall continue to work with the commercial space sector, including the Commercial Space Transportation Advisory Committee, to facilitate the development of voluntary consensus standards based on recommended best practices to improve the safety of

crew, government astronauts, and space flight participants as the commercial space sector continues to mature.''.

(b) BIENNIAL REPORT.—Beginning on December 31, 2016, and biennially thereafter, the Secretary of Transportation, in consultation and coordination with the commercial space sector, including the Commercial Space Transportation Advisory Committee, shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives a report detailing progress on the development of industry voluntary consensus standards under section 50905(c)(6) of title 51, United States Code.

SEC. 11. GOVERNMENT ASTRONAUTS.

(a) FINDINGS AND PURPOSE.—Section 50901(15) is amended by inserting '', government astronauts,'' after ''crew'' each place it appears.

(b) DEFINITION OF GOVERNMENT ASTRONAUT.—Section 50902 is amended—

(1) by redesignating paragraphs (4) through (22) as paragraphs (7) through (25), respectively; and

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

''(4) 'government astronaut' means an individual who—

''(A) is either—

''(i) an employee of the United States Government, including the uniformed services, engaged in the performance of a Federal function under authority of law or an Executive act; or

''(ii) an international partner astronaut;

''(B) is identified by the Administrator of the National Aeronautics and Space Administration;

''(C) is carried within a launch vehicle or reentry vehicle; and

''(D) may perform or may not perform activities directly relating to the launch, reentry, or other operation of the launch vehicle or reentry vehicle.

''(5) 'international partner astronaut' means an individual designated under Article 11 of the International Space Station Intergovernmental Agreement, by a partner to that agreement other than the United States, as qualified to serve as an International Space Station crew member.

''(6) 'International Space Station Intergovernmental Agreement' means the Agreement Concerning Cooperation on the International Space Station, signed at Washington January 29, 1998 (TIAS 12927).''.

(c) DEFINITION OF LAUNCH.—Paragraph (7) of section 50902, as redesignated, is amended by striking ''and any payload, crew, or space flight participant'' and inserting ''and any payload or human being''.

(d) DEFINITION OF LAUNCH SERVICES.—Paragraph (9) of section 50902, as redesignated, is amended by striking ''payload, crew (including crew training), or space flight participant'' and inserting ''payload, crew (including crew training), government astronaut, or space flight participant''.

(e) DEFINITION OF REENTER AND REENTRY.—Paragraph (16) of section 50902, as redesignated, is amended by striking ''and its payload, crew, or space flight participants, if any,'' and inserting ''and its payload or human beings, if any,''.

(f) DEFINITION OF REENTRY SERVICES.—Paragraph (17) of section 50902, as redesignated, is amended by striking ''payload, crew (including crew training), or space flight participant, if any,'' and inserting ''payload, crew (including crew training), government astronaut, or space flight participant, if any,''.

(g) DEFINITION OF SPACE FLIGHT PARTICIPANT.—Paragraph (20) of section 50902, as redesignated, is amended to read as follows:

''(20) 'space flight participant' means an individual, who is not crew or a government astronaut, carried within a launch vehicle or reentry vehicle.''.

(h) DEFINITION OF THIRD PARTY.—Paragraph (24)(E) of section 50902, as redesignated, is amended by inserting '', government astronauts,'' after ''crew''.

(i) RESTRICTIONS ON LAUNCHES, OPERATIONS, AND REENTRIES; SINGLE LICENSE OR PERMIT.—Section 50904(d) is amended by striking ''activities involving crew or space flight participants'' and inserting ''activities involving crew, government astronauts, or space flight participants''.

(j) LICENSE APPLICATIONS AND REQUIREMENTS; APPLICATIONS.—Section 50905 is amended—

(1) in subsection (a)(2), by striking ''crews and space flight participants'' and inserting ''crew, government astronauts, and space flight participants'';

(2) in subsection (b)(2)(D), by striking ''crew or space flight participants'' and inserting ''crew, government astronauts, or space flight participants''; and

(3) in subsection (c)—

(A) in paragraph (1), by striking ''crew and space flight participants'' and inserting ''crew, government astronauts, and space flight participants''; and

(B) in paragraph (2), by striking ''to crew or space flight participants'' each place it appears and inserting ''to crew, government astronauts, or space flight participants''.

(k) MONITORING ACTIVITIES.—Section 50907(a) is amended by striking ''crew or space flight participant training'' and inserting ''crew, government astronaut, or space flight participant training''.

(l) ADDITIONAL SUSPENSIONS.—Section 50908(d)(1) is amended by striking ''to crew or space flight participants'' each place it appears and inserting ''to any human being''.

(m) ENFORCEMENT AND PENALTY.—Section 50917(b)(1)(D)(i) is amended by striking ''crew or space flight participant training site,'' and inserting ''crew, government astronaut, or space flight participant training site,''.

(n) RELATIONSHIP TO OTHER EXECUTIVE AGENCIES, LAWS, AND INTERNATIONAL OBLIGATIONS; NONAPPLICATION.—Section 50919(g) is amended to read as follows:

''(g) NONAPPLICATION.—

''(1) IN GENERAL.—This chapter does not apply to—

''(A) a launch, reentry, operation of a launch vehicle or reentry vehicle, operation of a launch site or reentry site, or other space activity the Government carries out for the Government; or

''(B) planning or policies related to the launch, reentry, operation, or activity under subparagraph (A).

''(2) RULE OF CONSTRUCTION.—The following activities are not space activities the Government carries out for the Government under paragraph (1):

''(A) A government astronaut being carried within a launch vehicle or reentry vehicle under this chapter.

''(B) A government astronaut performing activities directly relating to the launch, reentry, or other operation of the launch vehicle or reentry vehicle under this chapter.''.

(o) RULE OF CONSTRUCTION.—Nothing in this Act, or the amendments made by this Act, may be construed to modify or affect any law relating to astronauts.

SEC. 12. STREAMLINE COMMERCIAL SPACE LAUNCH ACTIVITIES.

(a) SENSE OF CONGRESS.—It is the sense of Congress that eliminating duplicative requirements and approvals for commercial launch and reentry operations will promote and encourage the development of the commercial space sector.

(b) REAFFIRMATION OF POLICY.—Congress reaffirms that the Secretary of Transportation, in overseeing and coordinating commercial launch and reentry operations, should—

(1) promote commercial space launches and reentries by the private sector;

(2) facilitate Government, State, and private sector involvement in enhancing U.S. launch sites and facilities;

(3) protect public health and safety, safety of property, national security interests, and foreign policy interests of the United States; and

(4) consult with the head of another executive agency, including the Secretary of Defense or the Administrator of the National Aeronautics and Space Administration, as necessary to provide consistent application of licensing requirements under chapter 509 of title 51, United States Code.

(c) REQUIREMENTS.—

(1) IN GENERAL.—The Secretary of Transportation under section 50918 of title 51, United States Code, and subject to section 50905(b)(2)(C) of that title, shall consult with the Secretary of Defense, the Administrator of the National Aeronautics and Space Administration, and the heads of other executive agencies, as appropriate—

(A) to identify all requirements that are imposed to protect the public health and safety, safety of property, national security interests, and foreign policy interests of the United States relevant to any commercial launch of a launch vehicle or commercial reentry of a reentry vehicle; and

(B) to evaluate the requirements identified in subparagraph (A) and, in coordination with the licensee or transferee and the heads of the relevant executive agencies—

(i) determine whether the satisfaction of a requirement of one agency could result in the satisfaction of a requirement of another agency; and

(ii) resolve any inconsistencies and remove any outmoded or duplicative requirements or approvals of the Federal Government relevant to any commercial launch of a launch vehicle or commercial reentry of a reentry vehicle.

(2) REPORTS.—Not later than 180 days after the date of enactment of this Act, and annually thereafter until the Secretary of Transportation determines no outmoded or duplicative requirements or approvals of the Federal Government exist, the Secretary of Transportation, in consultation with the Secretary of Defense, the Administrator of the National Aeronautics and Space Administration, the commercial space sector, and the heads of other executive agencies, as appropriate, shall submit to the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Science, Space, and Technology of the House of Representatives, and the congressional defense committees a report that includes the following:

(A) A description of the process for the application for and approval of a permit or license under chapter 509 of title 51, United States Code, for the commercial launch of a launch vehicle or commercial reentry of a reentry vehicle, including the identification of—

(i) any unique requirements for operating on a United States Government launch site, reentry site, or launch property; and

(ii) any inconsistent, outmoded, or duplicative requirements or approvals.

(B) A description of current efforts, if any, to coordinate and work across executive agencies to define interagency processes and procedures for sharing information, avoiding duplication of effort, and resolving common agency requirements.

(C) Recommendations for legislation that may further—

(i) streamline requirements in order to improve efficiency, reduce unnecessary costs, resolve inconsistencies, remove duplication, and minimize unwarranted constraints; and

(ii) consolidate or modify requirements across affected agencies into a single application set that satisfies the requirements identified in paragraph (1)(A).

(3) DEFINITIONS.—For purposes of this subsection—

(A) any applicable definitions set forth in section 50902 of title 51, United States Code, shall apply;

(B) the terms ''launch'', ''reenter'', and ''reentry'' include landing of a launch vehicle or reentry vehicle; and

(C) the terms ''United States Government launch site'' and ''United States Government reentry site'' include any necessary facility, at that location, that is commercially operated on United States Government property.

SEC. 13. OPERATION AND UTILIZATION OF THE ISS.

(a) SENSE OF CONGRESS.—It is the sense of Congress that—

(1) maximum utilization of partnerships, scientific research, commercial applications, and exploration test bed capabilities of the ISS is essential to ensuring the greatest return on investments made by the United States and its international partners in the development, assembly, and operations of that unique facility; and

(2) every effort should be made to ensure that decisions regarding the service life of the ISS are based on the station's projected capability to continue providing effective and productive research and exploration test bed capabilities.

(b) CONTINUATION OF THE INTERNATIONAL SPACE STATION.—

(1) IN GENERAL.—Section 501 of the National Aeronautics and Space Administration Authorization Act of 2010 (42 U.S.C. 18351) is amended—

*(A) in the heading, by striking ''**THROUGH 2020**''; and*

(B) in subsection (a), by striking ''through at least 2020'' and inserting ''through at least 2024''.

(2) MAINTENANCE OF THE UNITED STATES SEGMENT AND ASSURANCE OF CONTINUED OPERATIONS OF THE INTERNATIONAL SPACE STATION.—Section 503 of the National Aeronautics and Space Administration Authorization Act of 2010 (42 U.S.C. 18353) is amended—

(A) in subsection (a), by striking ''through at least September 30, 2020'' and inserting ''through at least September 30, 2024''; and

(B) in subsection (b)(1), by striking ''In carrying out subsection (a), the Administrator'' and inserting ''The Administrator''.

(3) RESEARCH CAPACITY ALLOCATION AND INTEGRATION OF RESEARCH PAYLOADS.—Section 504(d) of the National Aeronautics and Space Administration Authorization Act of 2010 (42 U.S.C. 18354(d)) is amended by striking ''September 30, 2020'' each place it appears and inserting ''at least September 30, 2024''.

(4) MAINTAINING USE THROUGH AT LEAST 2024.—Section 70907 is amended to read as follows:

''§ 70907. Maintaining use through at least 2024

''(a) POLICY.—The Administrator shall take all necessary steps to ensure that the International Space Station remains a viable and productive facility capable of potential United States utilization through at least September 30, 2024.

''(b) NASA ACTIONS.—In furtherance of the policy under subsection (a), the Administrator shall ensure, to the extent practicable, that the International Space Station, as a designated national laboratory—

''(1) remains viable as an element of overall exploration and partnership strategies and approaches;

''(2) is considered for use by all NASA mission directorates, as appropriate, for technically appropriate scientific data gathering or technology risk reduction demonstrations; and

''(3) remains an effective, functional vehicle providing research and test bed capabilities for the United States through at least September 30, 2024.''.

(5) TECHNICAL AND CONFORMING AMENDMENTS.—

(A) TABLE OF CONTENTS OF 2010 ACT.—The item relating to section 501 in the table of contents in section 1(b) of the National Aeronautics and Space Administration Authorization Act of 2010 (124 Stat. 2806) is amended by striking ''through 2020''.

(B) TABLE OF CONTENTS OF CHAPTER 709.—The table of contents for chapter 709 is amended by amending the item relating to section 70907 to read as follows:

''70907. Maintaining use through at least 2024.''.

Mr. ROUNDS. I ask unanimous consent that the committee-reported substitute amendment be agreed to, the bill, as amended, be read a third time and passed, and that the motion to reconsider be considered made and laid upon the table.

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

The committee-reported amendment in the nature of a substitute was agreed to.

The bill (S. 1297), as amended, was ordered to be engrossed for a third reading, was read the third time, and passed.

GENERAL OF THE ARMY OMAR BRADLEY PROPERTY TRANSFER ACT OF 2015

Mr. ROUNDS. Mr. President, I ask unanimous consent that the Committee on Armed Services be discharged from further consideration of S. 267 and the Senate proceed to its immediate consideration.

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

The clerk will report the bill by title.

The senior assistant legislative clerk read as follows:

A bill (S. 267) to authorize the transfer of certain items under the control of the Omar Bradley Foundation to the descendants of General Omar Bradley.

There being no objection, the Senate proceeded to consider the bill.

Mr. ROUNDS. I ask unanimous consent that the bill be read a third time and passed and the motion to reconsider be considered made and laid upon the table.

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

The bill (S. 267) was ordered to be engrossed for a third reading, was read the third time, and passed, as follows:

S. 267

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''General of the Army Omar Bradley Property Transfer Act of 2015''.

SEC. 2. TRANSFER OF CERTAIN ITEMS OF THE OMAR BRADLEY FOUNDATION TO THE DESCENDANTS OF GENERAL OMAR BRADLEY.

(a) TRANSFER AUTHORIZED.—The Omar Bradley Foundation, Pennsylvania, may transfer, without consideration, to the child of General of the Army Omar Nelson Bradley and his first wife Mary Elizabeth Quayle Bradley, namely Elizabeth Bradley, such items of the Omar Bradley estate under the control of the Foundation as the Secretary of the Army determines to be without historic value to the Army.

(b) TIME OF SUBMITTAL OF CLAIM FOR TRANSFER.—No item may be transferred under subsection (a) unless the claim for the transfer of such item is submitted to the Omar Bradley Foundation during the 180-day period beginning on the date of the enactment of this Act.

EXPRESSING THE SENSE OF THE SENATE ON THE OBSERVANCE OF 1890 LAND-GRANT INSTITUTIONS QUASQUICENTENNIAL RECOGNITION DAY

Mr. ROUNDS. Mr. President, I ask unanimous consent that the Agriculture, Nutrition, and Forestry Committee be discharged from further consideration of and the Senate now proceed to the consideration of S. Res. 232.

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

The clerk will report the resolution by title.

The senior assistant legislative clerk read as follows:

A resolution (S. Res. 232) expressing the sense of the Senate that August 30, 2015, be observed as ''1890 Land-Grant Institutions Quasquicentennial Recognition Day.''

There being no objection, the Senate proceeded to consider the resolution.

Mr. ROUNDS. Mr. President, I ask unanimous consent that the resolution be agreed to, the preamble be agreed to, and the motions to reconsider be considered made and laid upon the table.

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

The resolution (S. Res. 232) was agreed to.

The preamble was agreed to.

(The resolution, with its preamble, is printed in the RECORD of July 27, 2015, under ''Submitted Resolutions.'')

ORDERS FOR WEDNESDAY, AUGUST 5, 2015

Mr. ROUNDS. Mr. President, I ask unanimous consent that when the Senate completes its business today, it adjourn until 9:30 a.m., Wednesday, August 5; that following the prayer and pledge, the morning hour be deemed expired, the Journal of proceedings be approved to date, and the time for the two leaders be reserved for their use later in the day; that following leader remarks, the Senate resume consideration of the motion to proceed to S. 754; finally, that the time following leader remarks until the cloture vote be equally divided between the two managers or their designees.

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

ADJOURNMENT UNTIL 9:30 A.M. TOMORROW

Mr. ROUNDS. Mr. President, if there is no further business to come before the Senate, I ask unanimous consent that it stand adjourned under the previous order.

There being no objection, the Senate, at 7:14 p.m., adjourned until Wednesday, August 5, 2015, at 9:30 a.m.