United States of America

Congressional Record

PROCEEDINGS AND DEBATES OF THE 112th CONGRESS, SECOND SESSION

Vol. 158 WASHINGTON, TUESDAY, JULY 31, 2012 *No. 115*

Senate

The Senate met at 10 a.m. and was called to order by the Honorable CHRISTOPHER A. COONS, a Senator from the State of Delaware.

PRAYER

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

Let us pray.

Creator God, who has nurtured us throughout the seasons of our sojourn, give to the Members of this body the love, strength, and wisdom to do Your will. Keep them walking in the paths of righteousness and let them feel Your abiding presence in times of joy and sadness. Lord, empower them to hold fast to the good will that unites them, making them instruments of Your purposes to bring peace in our days, peace to our souls, peace to our families, peace to our country, and peace among nations. May they be moved by Your majesty and motivated by the magnitude of the responsibilities You have entrusted to them.

We pray in Your mighty Name. Amen.

PLEDGE OF ALLEGIANCE

The Honorable CHRISTOPHER A. COONS 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.

APPOINTMENT OF ACTING PRESIDENT PRO TEMPORE

The PRESIDING OFFICER. The clerk will please read a communication to the Senate from the President pro tempore (Mr. INOUYE).

The legislative clerk read the following letter.

U.S. SENATE,
PRESIDENT PRO TEMPORE,
Washington, DC, July 31, 2012.

To the Senate:

Under the provisions of rule I, paragraph 3, of the Standing Rules of the Senate, I hereby appoint the Honorable CHRISTOPHER A. COONS, a Senator from the State of Delaware, to perform the duties of the Chair.

DANIEL K. INOUYE,
President pro tempore.

Mr. COONS thereupon assumed the chair as Acting President pro tempore.

RECOGNITION OF THE MAJORITY LEADER

The ACTING PRESIDENT pro tempore. The majority leader is recognized.

SCHEDULE

Mr. REID. Mr. President, we are already on S. 3414, which is the cyber security bill. The time until 2:15 p.m., is for debate only, and the time until 12:30 p.m. will be equally divided between the two leaders or their designees. The majority will control the first hour and the Republicans the second hour.

The Senate will recess from 12:30 p.m. until 2:15 p.m. for the weekly caucus meetings.

I will alert everyone to this: I hope those people, led by Senator LIEBERMAN and Senator COLLINS, will work to come up with a finite list of amendments so we can move on the cyber security bill.

I spoke to the Republican leader yesterday and have been very patient and tried to get a list of amendments we can agree on. I hope that can be done soon. It is very important that we make a determination of whether we are going to be able to get a bill. There is not a lot of time left to tread water, so to speak.

This is an important piece of legislation. All one needs to do is look at what is going on in India today. There are no cyber problems there that I am aware of, but one-half of the country of India is without electricity today. Transportation has been shut down, financial networks in India, which are significant, are down, and it is a chaotic place. There are 600 million people in India who are without electricity. As we have been told time and time again, the most important issue we have facing this country today for security is cyber. We have been told that by the Joint Chiefs of Staff and by the head of the CIA. We have been told that by Democrats and Republicans. It is an issue that is important, and we have been told it is something we can prevent.

If we don't do this bill, it is not a question of if there will be a cyber attack that will be devastating to our country, it is only a question of when. It can be stopped. I hope the chamber of commerce will get some sense.

There was a big meeting in the Chamber yesterday. They were moving forward on all that was bad about the bill. The problem is they were dealing with the wrong bill. So I hope we can get something done. It is extremely important that we do.

There will be a Senators-only briefing today at 5 p.m. in the Visitor Center today in SVC–217.

MEASURES PLACED ON THE CALENDAR—S. 3457 AND H.R. 4078

Mr. REID. I am told there are two bills at the desk due for a second reading.

The ACTING PRESIDENT pro tempore. The Senator is correct. The clerk will report the bills by title for the second time.

The legislative clerk read as follows:

A bill (S. 3457) to require the Secretary of Veterans Affairs to establish a veterans job corps, and for other purposes.

A bill (H.R. 4078) to provide that no agency may take any significant regulatory action until the unemployment rate is equal to or less than 6.0 percent.

Mr. REID. Mr. President, I object to any further proceedings with regard to these bills at this time.

The ACTING PRESIDENT pro tempore. Objection is heard. The bills will be placed on the calendar.

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

AFFORDABLE CARE ACT

Mr. REID. Mr. President, I am going to spend a few minutes talking about the Affordable Care Act. I wonder how many people on the Republican side today are going to talk about ObamaCare. If they do, they should be in a very positive state. We know that as a result of this bill, the Affordable Care Act, people are getting or soon will get a rebate. One of the things we did—led by Senator FRANKEN and others—was make sure that 80 percent of the money paid for premiums goes to patient care and any amount that doesn't has to be refunded to the patients. That is in the process now. In the month of August, all those moneys will come back in a significant amount to Americans who, in effect, are part of programs that spend too much on salaries for bosses.

Also, we are going to talk a little bit today about what this Affordable Care Act does for women in America. As I said, I am going to speak very briefly, but we are going to have people come—as soon as I and the Republican leader finish—to talk about good things in this bill for women. I will touch on them very briefly.

There is no question this bill that was signed by President Obama is a landmark piece of legislation. It signaled an end to insurance company discrimination among many but especially against those who are ill, those with a preexisting condition, and especially against women.

As a result of this bill we passed, being a woman is no longer a preexisting disability in America. For many years, insurance companies charged American women higher premiums. Why? Because they are women. For years, American women have unfairly borne the burden of the high cost of contraception as well. Even women with private insurance often wind up spending hundreds of dollars more each year for birth control. Today, women of reproductive age spend two-thirds more out of their own pockets for health care costs than men, largely due to the high cost of birth control. But starting tomorrow—Wednesday of this week—new insurance plans must cover contraception and many other preventive health services for women. How much? No additional pay at all. Under health care reform, about 47 million women, including almost 400,000 women in Nevada, will have guaranteed access to those additional preventive services without cost sharing.

Many on the other side downplayed the importance of these benefits or fought to repeal them altogether. It is hard to comprehend but true. Forcing American women to continue struggling with the high price of contraception has very real consequences. Every year millions of women in the United States put off doctors' visits because they can't afford the copay and millions more skip pills or shots to save money.

It is no mystery why the United States has one of the highest rates of unintended pregnancies of all industrialized nations. Half of all pregnancies in America are unplanned. Of those unintended pregnancies, about half wind up in abortion. Increasing access to contraception is the most effective way to reduce unintended pregnancies and reduce the number of abortions, but the high cost is often a barrier.

That is why, in 1997, OLYMPIA SNOWE and I began a bipartisan effort to prevent unintended pregnancies by expanding access to contraception. It has not been an easy path, but we did make a start. As part of this effort, we helped pass a law ensuring Federal employees access to contraception. It was a big issue. That was 15 years ago or more. It is an issue that is still important, but we started it, and I am very happy about that. OLYMPIA SNOWE was terrific to work with.

When this benefit took place in 1999, premiums did not go up one single dime because neither did health care costs—not one penny. It was rewarding to note that a pro-life Democrat and pro-choice Republican were able to confront the issue with a practical eye rather than a political eye. It is unfortunate that over the last 15 years an idea that started as a common-ground proposal has become so polarizing in Congress. The controversy is quite strange when we consider that almost 99 percent of women have relied on contraception at some point in their lives, and many have struggled to afford it. The Affordable Care Act will ensure that insurance companies treat women fairly and treat birth control as any other preventive service.

Prior to Senator SNOWE and me doing this, anything a man wanted they got. Viagra, fine; we will take care of that. Anything a man wanted they got—but not a woman. The law doesn't just guarantee women's access to contraception, it assures their access to many other lifesaving procedures as well.

Thanks to the health care bill—the Affordable Care Act—insurance companies are already required to cover preventive care such as mammograms. For a person who is able to have a mammogram, it is lifesaving. Most people in the Senate know my wife is battling breast cancer. She had a mammogram in December and in August discovered a lump in her breast. Think of what would have happened if she had waited 1 year because she couldn't afford that mammogram. Frankly, the thought of it is very hard for me to comprehend because even though she had that mammogram in December, she had found it and was in stage 3 of breast cancer. It has been very difficult. What if she waited an extra year? Many people wait a lot longer than an extra year.

Colonoscopies save lives. I was talking to one of my friends in the Senate who is going to have his done. They do it every 5 years. It takes at least 10 years for polyps to develop into cancer, and some polyps develop into cancer if they are not taken out. People need to have this done.

Blood pressure checks, childhood immunizations without cost sharing is part of what is in this bill. It used to be a bill; now it is the law.

Starting tomorrow—again, Wednesday of this week—women will no longer have to reach in their pockets to pay for wellness checkups. They can do screening for diabetes, HPV testing, sexually transmitted infection counseling, HIV screening and counseling, breastfeeding support, domestic violence screening and counseling. That is all in the law starting tomorrow. All women in new insurance plans will have access to all forms of FDA-approved contraception without having to shell out more money on top of their premiums. Ending insurance company discrimination will help millions more women afford the care they need when they need it. It will restore basic fairness to the health care system. Sometimes the practical thing to do is also the right thing to do, and that is what the legislation we worked so hard to pass is all about. It is about doing the right thing for everyone. Today we are going to focus on women.

RECOGNITION OF THE MINORITY LEADER

The ACTING PRESIDENT pro tempore. The Republican leader is recognized.

REPEAL OF OBAMACARE

Mr. MCCONNELL. Mr. President, I might say to my friend the majority leader before he leaves the floor that I listened carefully to his speech about what most Americans refer to as ObamaCare. Given the fact that our friends on the other side are going to focus on that bill this particular week, I think it might be a good idea to have a vote on it, on the pending bill.

It would be my intent to offer an amendment that I know my friend does not support, but nevertheless many Americans would like to know. Since we have spent a good deal of time positioning over the last few months on various and assorted issues, I think it would be appropriate to have a vote on the repeal of ObamaCare, and I hope to be able to offer that amendment during the pendency of the bill on cyber security, which we believe will be open to amendments. I wonder if my friend thinks that might be something both sides might agree would be a good idea.

Mr. REID. Mr. President, I wonder if the official reporter could show the big smile on my face. Can my colleagues imagine how ridiculous my friend the Republican leader's statement is. Listen to what he said. We are doing cyber security. We have talked about the dangers of cyber security if we don't do something about it. He is now telling me he wants a vote to repeal all the stuff I just talked about on the cyber security bill? That is very difficult to comprehend.

I think we should understand that I don't think a woman getting contraception has a thing to do with shutting down the power grids in America or the financial services in America or our water systems or our sewer systems. That is what cyber security is all about, not whether a woman can have contraception or whether she can have a wellness check to find out if she has cancer from not having had a mammogram.

Mr. DURBIN. Mr. President, will the majority leader yield for a question?

Mr. REID. I would be happy to yield.

Mr. DURBIN. I would like to ask the majority leader, do I remember correctly that the very first amendment on the Transportation bill was offered by Senator BLUNT of Missouri on family planning? So is there a family planning amendment available on every bill now that will be offered by the Republican side?

I know the House Republicans have had 30 or 33 votes to repeal ObamaCare. Are we going to try to match them with similar efforts in the Senate?

Mr. REID. My response to my friend is this: I try to be very calm about things in life generally, especially things here on the floor, but I can't remain very calm about this. I have, as do a lot of people I know, 16 grandchildren. They are evenly divided between boys and girls. I want my granddaughters to be treated so that if they want to go get some contraception, have some contraceptive device while in school at New York University or Berkeley—I am bragging that they got into those schools—they should have the ability to do that.

I just can't imagine what we are talking about here on the Senate floor. Cyber security is one of the most important—it is the most important issue, as I have already said. If my colleagues want to talk to General Petraeus, he will tell us about what it is, or General Dempsey will tell us what the important issue is. The No. 1 issue today is whether we are going to have bad people attack our country and shut it down. Now we are here being asked if we are going to have a vote, on cyber security, as to when my grandchildren can have contraception.

The ACTING PRESIDENT pro tempore. The Republican leader.

Mr. MCCONNELL. I guess the answer is no.

My friends are going to spend the week lauding the advantages as they see them of an immensely unpopular bill that was passed a couple of years ago on a straight party-line vote—ObamaCare. Yet, in a week in which, apparently, they are going to laud the various positions of it, they are not willing to have a vote in support of it. So I gather that is a vote we will not have. I will request the opportunity to do that again. After listening to my good friend the majority leader, I anticipate such a request would likely be blocked.

On another matter——

Mr. REID. Mr. President, my friend asked me a question.

Mr. MCCONNELL. I believe I have the floor.

The ACTING PRESIDENT pro tempore. The Republican leader has the floor.

Mr. REID. OK. I won't answer the question then.

DEFENSE SEQUESTER

Mr. MCCONNELL. Mr. President, 4 years after the great recession began, millions of Americans are still looking for work, millions more have literally dropped out of the workforce altogether, and uncertainty about our Nation's future continues to spread. The stories of disappointment and of loss haven't diminished; they have, in fact, multiplied.

What is worse, a President who was elected on a pledge that he would turn all those things around is still pointing the finger at his predecessor. Three and a half years after he took office, he is acting as though he just showed up. I think most Americans are smart enough to know he has made things worse. He has hammered small businesses with a barrage of new regulations, with dozens more in the pipeline. He expects them to plan for the future without even knowing what their tax and health care liabilities will be. Last week he even spearheaded a legislative effort to take even more of what nearly 1 million of these small businesses earn, and then he told Republicans that if we don't go along with it, he will raise taxes on everybody else.

That was the message last week: Either give me what I want—raise taxes on 1 million of our most successful small businesses—or we will let everybody's taxes go up, is what he said at the end of the week. In other words, he used small businesses as little more than a bargaining chip. The week before that he told business owners that they are not really responsible for what they have built. Listen to that. To business owners, the President said: You are not really responsible for what you have built. No amount of White House spin or manufactured outrage can change what the President said in Roanoke, and no amount of finger-pointing can change the fact that his policies have actually made things worse.

But what is most upsetting to a lot of us is the fact that the administration pretends its policies would help the economy or create jobs when it knows they won't. It knows these policies are not going to create any jobs. What is most upsetting is the deception that lies at the heart of so many of the sales jobs, from health care to the stimulus.

Americans wanted the President to focus on jobs, and he focused on a health care bill that we now learn not only includes a tax on the middle class but will lead to hundreds of thousands of fewer jobs. Now the President claims he is fighting for the middle class, but 3½ years into his Presidency their wages are still stagnant while their dependency on government assistance actually continues to rise. Wages are stagnant, and dependence on government assistance continues to rise.

In some cases the President doesn't even bother with the sales jobs; he just keeps his plans a secret. That is what we are now seeing with the defense cuts he demanded during last year's budget negotiations. Literally for weeks, Republicans asked the President to tell the American people how he planned to carry out these cuts. He refused.

Mr. President, the Senate is not in order.

The ACTING PRESIDENT pro tempore. The Senate will be in order.

The Republican leader.

Mr. MCCONNELL. As I was saying, for weeks Republicans asked the President to tell the American people how he plans to carry out these cuts. He simply refused to do so. So last week Congress passed legislation requiring him to do so. In fact, it cleared the Senate, I believe, unanimously.

Then yesterday there was this: An Assistant Secretary down at the Department of Labor is now telling people they are under no legal obligation to let employees know if they will lose their jobs as a result of these cuts. Let me say that again. We have an Assistant Secretary of Labor who just yesterday said that employers are under no legal obligation to tell their employees they may lose their jobs as a result of these cuts. In other words, the President is trying to keep those folks in the dark about whether they can expect to lose their jobs. Why? Well, I think it is pretty obvious: to insulate himself from the political fallout that will result. The President doesn't want people reading about pink slips in the weeks before his election, so the White House is telling people to keep the effects of these cuts a secret—don't tell anybody, he says, keep it a secret—until, of course, after the election. Once again, a President who holds himself out as a great defender of the middle class and the goals of organized labor is putting his own political goals ahead of the hard-working Americans who will be affected by these policies. Rather than let those who will be affected by the cuts know about them, he will make everybody nervous.

For 3½ years—3½ long years—this President has pushed an ideological agenda without regard for the consequences it would have on the very middle-class Americans he purports to defend.

The President may not want to admit it, but the economic mess we are in is his legacy—his legacy. After 3½ years of finger-pointing—3½ years of finger-pointing—he owes it to the American people to be straight about it.

Mr. President, I yield the floor.

CYBERSECURITY ACT OF 2012

The ACTING PRESIDENT pro tempore. The clerk will report the pending business.

The legislative clerk read as follows:

A bill (S. 3414) to enhance the security and resiliency of the cyber and communications infrastructure of the United States.

The ACTING PRESIDENT pro tempore. The Senator from Maryland.

Ms. MIKULSKI. Mr. President, every Senator has to decide what they are going to do every day when they wake up in the morning. For some in this Chamber, they wake up every day thinking about how they are going to stop President Obama, how they are going to stop his agenda, and how they are going to do everything they can to stop him from having a second term. Some spend their time waking up every day thinking about how they want to stop America from moving forward.

That is not how I spend my day. I try to look at two things every day: the needs of my people—their day-to-day needs for a job, for an opportunity, for health care—and how that translates into national policy; then I try to look at the long range needs of our country. That is why I am excited about being on the Intelligence Committee, where I am working on protecting America from the cyber attacks that are happening every day to our country, including the stealing of identity and the stealing of trade secrets. I want to move America forward. I have worked very hard to do that.

One of the areas I am most proud of that I have worked on with the men and women in this Chamber from both sides of the aisle is the whole area of women's health care. Many want to talk about repealing Obama health care. Well, I don't want to repeal it. They talk about replacing it. They never have an idea. So let me tell my colleagues one of the areas we fought for.

One of the things we knew as we embarked upon the health care debate was that we wanted to save lives and we wanted to save money. One of the areas where we wanted to do both was to look at how to utilize the new scientific breakthroughs in prevention, particularly early detection and screening. We could identify those diseases with early intervention and save lives as well as money and counteract escalating disease that ultimately costs more and can even cost a life.

Nowhere was it more glaring than with the issue of women's health care. My hearings revealed that women were charged more for their health care and got less than men of equal age and health care status. We found that we had barriers to health care because everything about being a woman was treated as a preexisting condition. If a woman had a C-section for the delivery of her baby, that was counted. In eight States, they even counted domestic violence as a preexisting condition. Then what we saw during this debate was the fact that they even wanted to take our mammograms away from us. Well, that just went too far.

So during the health care debate, while everybody was being a bean counter, I wanted American women to know they could count on the Senate and the women and men of the Senate to stand up for them. So we came to the floor. We suited up, and we fought for a preventive health care amendment that not only passed but goes into effect tomorrow, on August 1. It will be a new day for women of all ages, who will be able to get health care coverage for preventive health care at no additional cost, no copays, no deductibles, and no discrimination where they are charged more and get less. That is what ObamaCare is. If somebody wants to repeal that, then bring it on. We are ready to fight. We want to fight for that annual health care checkup that will involve mammograms, Pap testing, and pelvic exams. We want to be able to do the screening for that dread ''C'' word, for colorectal cancer and lung cancer. We want to make sure that if a person thinks they are possibly a victim—a doctor suspects domestic violence—we can screen and counsel. We want women to be able to have that access, to be able to know early on what are those illnesses they are facing.

August 1 means our long-fought battle will actually go into effect. Where does it go into effect? Well, it is already in effect on the Federal law books. Now it will go into effect in doctors' offices. Women will have access to the health care their doctor says they need, not what an insurance company says they need or what some right-winger wants to take away from them.

We are pretty mad about this. We were mad 2 years ago when they wanted to take our mammograms away from us, and we are going to be pretty mad if they try to take our health care away from us. But what we are happy about—what we are happy about—is that for over more than 50 million American women tomorrow it will be a new day. They will be able to walk into their doctor's office. In the doctor's office they will say: Good morning. Can I help you? And when they say: When was the last time you had a mammogram, and the patient says: Well, I never had one because I could not afford it, they will say: Oh, we can sign you right up for that. Tell me about your family history. Is it true that your father had colon cancer? Well, listen, we worry about that for you. You could be at high risk. We are going to take a look at that and make sure you are OK.

For young women, we are going to make sure you have other kinds of counseling and services you need in order to have a productive family life. This is what this health care bill is all about. It is about people. It is about access. It is about preventing dread diseases.

People will come to this floor and they will pound their chest and complain about the President. We want to pound the table and make sure women have gotten the health care they need.

Tomorrow, we are going to be very excited when we keep the doors of doctors' offices open to the women of America.

Mr. President, I yield the floor.

The ACTING PRESIDENT pro tempore. The Senator from New York.

Mr. SCHUMER. Mr. President, first, I wish to give two thank-yous: first, to my colleague from California for letting me go ahead of her—I have a Finance Committee meeting—and second, to both my colleague from Maryland and my colleague from California, whose voices are so clear and clarion. I love to listen to the Senator from Maryland. She speaks right to the people. She has it. She gets it. And do you know what. If we could get every American in a giant football stadium and they could listen to Senators MIKULSKI and BOXER on health care, 80 percent would be for it. So I want to salute them and salute particularly Senator MIKULSKI for putting both the event earlier today and these speeches together.

I heard the minority leader speak, and it meant two things. First, it meant the Republican party does not want to do cyber security. It means the greatest threat to our Nation—probably even greater than terrorism, if you speak to some of our intelligence and military experts—will not be dealt with because we know what he is doing. He is asking for an unreasonable demand, unrelated to cyber security, to go on the floor, knowing that will stop us from moving forward.

It is a sad day. We have some of our colleagues from the other side of the aisle talking about that we must not abandon defense. Well, one of the strongest things the defense of our Nation needs is a strong cyber security bill. Because special interests—the Chamber of Commerce and others—do not want it, even though every military and intelligence leader has said how vital it is, it seems the other party's tea leaves show that the other party is going to block us from going forward. It is unfortunate and it is sad.

Then, second, the way he chose to block cyber security could not be worse in terms of substance and in terms of timing. Today, July 31, the minority leader wants to put on the floor the repeal of so many things that are going to happen tomorrow to women and to men across America that benefit them. So his timing could not be worse. The very day before we are going to see huge benefits for the American people, he wants us to debate repeal. Why don't we let the American people see the good parts of health care before we repeal it. And we are not going to repeal it.

I want to talk about this day—or tomorrow, actually—where so many portions of the Affordable Care Act go into effect.

Three million women in my home State of New York will benefit. From

Buffalo to Montauk, in Albany and in Manhattan, 3 million women will receive free basic preventive care for themselves and their children. So many women and men do not get preventive services because it is expensive to them. These services are free. But not only will they make those people healthier—the No. 1 goal—but they will reduce the costs of health care because every expert—Democrat, Independent, Republican; moderate, liberal, conservative—says if you do more prevention, you are going to save money.

Tomorrow, so many of those preventive services go into effect. More women will go in for annual preventive care visits to screen for cervical, ovarian, and breast cancers. More women will receive preconception and prenatal services, so their children can grow up healthy, active, and strong. More women will have access to contraception and its additional health benefits, such as reduced risk of breast cancer and protection against osteoporosis.

New mothers will have access to support and supplies for breastfeeding, and more women will be screened for domestic and sexual violence, sexually transmitted infections, and HIV.

To my colleagues on the other side of the aisle: When we say there is a war against women and they get their backs up—they want to repeal this and put nothing in its place, no preventive services, no access to contraception, none of the things I have mentioned—yes, it is a war on women. Because if they cared about women and they did not like ObamaCare, they would still have a proposal on the floor to keep these fine pieces of the legislation going forward so they are not cut off tomorrow, which is what they intend to do, but, of course, thank God, will not happen.

The change we are making helps every woman—who said: I would but I cannot afford it; it is just too expensive—finally get health care.

Removing the copays is a great thing. Cutting the costs of preventive care is something we long wished to do in America and can happen tomorrow.

What about all the other benefits that affect men and women alike: 2.5 million young adults who can stay on their parents' insurance; 5.2 million seniors—men and women—in the doughnut hole who save $3.7 billion on prescription drugs?

What about the idea that when your insurance company charges you too much, the money goes to profits and salaries and trips and advertising and not enough goes to health care? Starting tomorrow, you can get a rebate. We know our colleagues on the other side of the aisle—to them that is anathema, to make insurance companies give people a rebate.

So bottom line: We want to move forward on a cyber security bill, and we regret that the leader is putting logs in its way. And even more importantly, we want benefits to millions of women and millions of men to go forward, as was intended, as was voted for, as is the law of the land, and we will not let them deter us from bringing people those benefits.

I yield the floor.

The ACTING PRESIDENT pro tempore. The Senator from California.

Mrs. BOXER. Mr. President, I thank the Senator from New York for putting this into context for America.

What has happened here this morning is, instead of celebrating with us because tomorrow, August 1, an entire list of preventive services for women goes into effect because of ObamaCare—yes, our health care law—the Republican leader says he wants to repeal all those benefits.

Not only does the Republican leader, on behalf of the Republican minority, want to repeal the benefits that go into effect tomorrow for women, he wants to repeal the entire health care bill. He wants to have an amendment to the cyber security bill—which is so critical to our national security—he wants to put an amendment on there to repeal a law that the U.S. Supreme Court found was constitutional and whose benefits are beginning to take hold in this country, benefits that mean right now people are receiving refund checks in the mail because their insurance company overcharged them, and under ObamaCare you cannot do that, and hundreds of millions of dollars are going out to our people. The Republicans want to, I assume, force those people to send back their refunds because they want to repeal ObamaCare.

Look at the list of preventive health benefits I have on this chart that are already in effect because of the legislation. Already because of health reform—and I see Senator HARKIN in the Chamber, who shepherded this through, as our dear friend Ted Kennedy became sicker and sicker with brain cancer. I will never forget how Senator HARKIN stepped up to the plate, Senator Dodd stepped up to the plate, Senator MIKULSKI stepped up to the plate, and they were the lieutenants who got it done. And the Republicans want to take it away. I can only imagine how Senator HARKIN feels, having been in that fight. But I am here to say I am your supporter. I know what you did.

I know my people in California—the largest State in the Union—are getting breast cancer screenings now, with no copays. They are getting cervical cancer screenings, hepatitis A and B vaccines, measles and mumps vaccines, colorectal cancer screenings, diabetes screenings, cholesterol screenings, blood pressure screenings, obesity screenings, tobacco cessation, autism screenings. How important is that? In my State, they say there is an epidemic of autism. They are getting hearing screenings for newborns, sickle cell screenings for newborns, fluoride supplements, tuberculosis testing for children, depression screenings. How important is that? They are getting osteoporosis screenings. I watched as my mother was in agony from osteoporosis. There are things you can do now to avoid it. But you need the screening. You need to know whether those bones are losing their density. They are getting flu vaccines for children and the elderly.

This list goes into effect tomorrow. So let's take a look at the list that goes into effect tomorrow that my Republican friends want to repeal today.

Tomorrow, women will get access to all of these things without copays or coinsurance: contraception, well-woman visits, STD screenings and counseling, breastfeeding support and supplies, domestic violence screenings, gestational diabetes screenings, HIV screenings, and HPV testing.

I am stunned that on the eve of the broadest increase in benefits in my lifetime, the Republicans want to repeal these benefits for women. This is a continuation on their part of the war on women. They can get up and stand on their head and deny it and everything else. How else can you explain why, on the eve of the day that women are going to get all these benefits, they want to now cancel ObamaCare and stop all this from happening?

If you think it does not matter—let me say to you, Mr. President, I know you know it matters whether women get free contraception to cut back on unintended pregnancies and abortion and well-woman visits and breastfeeding support. How about domestic violence screenings—so critical. Some women are in these terrible relationships, and they go to the doctor, and they say: Well, I do not want to talk about it. Doctors will be taught how to spot domestic violence, and there can be an intervention that will save lives.

So here we stand. We have this list of benefits, women's preventive health benefits, that are going to go into effect tomorrow.

We are here to celebrate that. And instead of our Republican colleagues coming on the floor and joining us and saying how wonderful this is, and by the way, at the end of the day this saves money—we all know that. We all know it saves money when you have screening and counseling for STDs and you head off an illness. We all know it saves money. The health care bill saves money, and it reduces the deficit because of this investment in prevention. I cannot think of a more ridiculous situation than after a bill has become law for how many years now, Senator HARKIN? Is it a couple of years since we passed it? Years. It went to the Supreme Court. It was upheld. And now, just as we are about to see these great benefits for women go into place, the Republican leader says: Let's repeal ObamaCare today. Let's have an amendment on the cyber security bill, he said, to repeal the entire health care law.

The House voted 33 times, at least, to repeal it. So I am wondering, what is with this idea of repealing? Do you want to take away these benefits from

women? From children? From men? From families? Yes, I guess you do. I guess you stand for going back to the old days when people could hear from their insurance company that they were cut off, when insurance companies could spend 70 percent on themselves, on their own perks, and CEOs getting hundreds of millions of dollars and you, the patient, getting hardly anything. They want to go back. They want to take away the refunds. They want to take away the funding our seniors are getting as they deal with the high cost of prescription drugs. And we fixed that in this bill.

So I have to say, we make an investment in prevention, in keeping people healthy. We make sure being a woman is not a preexisting condition. And the Republicans today have relaunched their war against women. They are holding up the Violence Against Women Act that we passed over here in a bipartisan way. They will not take up the Senate bill and pass it. Why? They want to take away coverage in that bill from 30 million Americans.

They do not care about the immigrant population, obviously, the most vulnerable women there. They do not care about the college students, apparently. Because we get extra protections for them on college campuses. We protect the LGBT community. Clearly they are not interested in that. And they are not interested in protecting the Native American women.

So while the Speaker says: Oh, I will send conferees to a nonexistent conference on the Violence Against Women Act, he could simply pass the bill and make sure everyone is protected. Instead of celebrating today because women are getting all these wonderful benefits without a copay, they want to repeal all these benefits. They want to repeal this law.

Truly, I do not know what motivates them. I do not speak for them. But if they say it is to save money, that is simply not true. Because this bill saves money. This law saves money. Because we are investing in prevention. So the only thing I can think of is they want to hurt this President.

The Republican leader said his highest priority was making sure that President Obama is a one-term President. So I guess if it means attacking the health care law to hurt this President, he is willing to do it and hurt all my constituents who are getting these benefits and all of our constituents who are getting these benefits, hurting the American people.

Well, I say put politics aside. Let's see the Republicans come down here and celebrate the fact that finally our people are getting the health care they deserve and that they pay for.

I yield the floor.

The ACTING PRESIDENT pro tempore. The Senator from New Hampshire.

Mrs. SHAHEEN. Mr. President, I am proud to join my colleagues on the floor today—I thank Senator BOXER and Senator HARKIN for their leadership—just as I was proud back in December of 2009 to join Senator MIKULSKI in sponsoring the women's health amendment to the Affordable Care Act.

We are here today celebrating the fact that tomorrow, August 1, women will have access to important health services at no cost. Senator BOXER showed very clearly what a number of those preventive services are. Thanks to the provisions of the Affordable Care Act that go into effect this week, women will have access to a broad range of preventive services from well woman and prenatal visits to gestational diabetes screening, and they will have access to those services without copayments or deductibles. So finances will no longer stand in the way of women getting the preventive health care they need.

This also has the potential to save our health system money in the long run. The Centers for Disease Control estimates that 75 percent of our health care spending is on people with chronic diseases. So by taking these preventive measures, we can slow this growth and the associated cost of disease.

One of those preventive measures I want to talk about this morning is screening for gestational diabetes. As cochair of the Senate Diabetes Caucus, I understand the importance of gestational diabetes screening and the impact it can have on both the mother and the baby. Gestational diabetes affects almost 18 percent of all pregnancies in the United States. Unfortunately, the number of those cases is increasing. The consequences of gestational diabetes are real. Not only are there significant health effects for the mother and baby during pregnancy, but researchers have found that both the mother and baby may be at risk for developing type 2 diabetes later in life. By getting screened, both the mother and child can be alerted to potential long-term health risks.

I want to tell the story of one of my constituents, Megan from Panacook, NH, because she is a great example of why this screening is so important. During her 28th week of pregnancy, Megan was diagnosed with gestational diabetes. The screening she had alerted her to the potential related health issues and they allowed her to get the necessary treatment. I am happy to report that Megan gave birth to a healthy baby girl, Grace. She is now 8 weeks old. Under the Affordable Care Act, all pregnant women will now be able to receive the gestational diabetes screening for free.

Tomorrow also marks an important milestone in women's health for another preventive service. Women, beginning tomorrow, will have access to contraception at no cost. Birth control is something that most women use, and it is something the medical community believes is essential to the health of a woman and her family. For some 1.5 million women, birth control pills are not used for contraception but for medical purposes. They can reduce the risk of some cancers. With costs as high as $600 a year, birth control can be a serious economic concern for many women. Being able to now receive birth control for no cost will bring financial relief to so many of those women.

Again, I have a story of a young woman from New Hampshire who I think illustrates so clearly why these are such important provisions. Keri Wolfe from Swanzey, NH, is a full-time graduate student at Dartmouth. She is going to benefit from this provision because Keri takes birth control as a medical necessity for treating a health issue that affects her adrenal gland. While Keri is lucky to have insurance, she has to pay her plan's full deductible and then a monthly copay for her birth control. As a student who is trying to balance academic and living expenses, her prescriptions come at a significant cost annually. When her new insurance plan goes into effect, Keri is going to be able to get the full price of her birth control covered. That is great news in making sure she gets the health care she needs.

As Governor of New Hampshire, I was proud to sign legislation that required insurance companies to provide contraceptive coverage to women with no religious exemption. At that time it was understood by people on both sides of the aisle of all religious faiths that requiring contraceptive coverage was about women's health, and it was a basic health care decision. Yet over the last several months, opponents have continued to roll back contraceptive coverage at both the State and Federal level. Every woman should be able to make her own health care decisions. She should not have to have her boss stand in the way. The provisions that go into effect tomorrow ensure that women can make these decisions.

I thank Senator MIKULSKI and Senator HARKIN for their leadership on women's health. I join them in celebrating these important provisions that are going to make a huge difference for women's health, that are going to be good for women, for families, and for everyone in this country.

I yield the floor.

The ACTING PRESIDENT pro tempore. The Senator from Iowa.

Mr. HARKIN. Mr. President, first of all, let me commend the Senator from New Hampshire for her great leadership as a Governor and as a Senator in this whole area of health care for women especially. She is providing great leadership in this area, continues to provide that leadership. I want to join with the Senator from New Hampshire in saying we are not going to let these provisions that now are expanding coverage for so many women—47 million women in America—we are not going to let these roll back. We are not.

Again, if the people of this country elect Mr. Romney to be President and they turn over the Senate to the Republicans, there it goes. It is gone. It is

gone. I did not hear this this morning, but I understand the Republican leader said this morning—I stand to be corrected. As I understand, he said they wanted the first amendment that would be offered on the cyber security bill that I think is now before the Senate—he wanted the first amendment to be a repeal of the Affordable Care Act.

What timing. What timing, I say to the Republican leader. On the eve of when we are expanding preventive health care services for 47 million women in America, the Republican leader gets up and says: We want to vote to repeal this tomorrow. Tomorrow. Repeal it tomorrow.

Does that not kind of give you some idea of how they feel about the women of America and the health care of our mothers, our sisters, our daughters? That is what they want.

We have already voted 33 times to repeal portions of the health care act. I think we voted twice in the Senate to repeal the whole thing. They want to have another vote. I think it is more than curious that the Republican leader wants to vote to repeal it on the very day when we are expanding health care coverage for the women of America. Interesting.

Tomorrow is an important day for American women, thanks again to key provisions of the Affordable Care Act. I do want to commend Senator MIKULSKI for her great leadership in this area, Senator Dodd, Senator BINGAMAN. Senator Kennedy, when he became ill, asked us to take the leadership on different provisions of the Affordable Care Act on the HELP Committee and to get it through.

We had wonderful support from our colleagues here on the floor of the Senate and our committee. These provisions that we put in to move us from a sick care system to a health care system—I have often said that in America we do not have a health care system, we have a sick care system. If you get sick, you will get care one way or the other, usually in the emergency room if you are poor, or maybe not at all if you do not make it to the emergency room. But there is very little in our country to keep you healthy in the first place. Yet we know, we have good data that shows preventive services upfront save you a lot of money and a lot of lives, a lot of pain and suffering later on. So in the Affordable Care Act we put in a big provision on preventive services. We said basically that what the Preventive Services Task Force of the Center for Disease Control and Prevention—what they listed as their A and B, those that had the, if I can use their term, ''best return on investment'' or the ''biggest impact,'' that those would be free, there would be no copays or deductibles.

Senator MIKULSKI reminded us of what is obvious but not too often taken into consideration in legislation; that is, women are different from men. So we asked the Institute of Medicine to come up with provisions that applied to the preventive health care of women. That is what goes into effect tomorrow.

Senator BOXER very eloquently talked about that and had the chart showing all of the different things that will start tomorrow—an all-new plan that would cover women in this country—again, to keep women healthy in the first place, preventive services to keep women healthy without copays and deductibles.

Right on the eve of this wonderful expansion of health care coverage, of making sure women are not second-class citizens when it comes to prevention and wellness—on the very eve of saying to women that no longer can insurance companies sort of say, because you are a woman you have a preexisting condition—the Senate Republican leader gets up and says he wants to have the next vote on repealing the health care bill.

Talk about a slap in the face to the women of this country. Well, I think women know what they are facing coming up this fall. I point out that tomorrow about 520,000 women in Iowa will have expanded health care coverage, preventive services. We fought very hard to put these into law, and we are not going to let them repeal it. We have the votes—let's face it—in the Senate to stop that. The Republican leader can bring it up again, and it can be voted on, but I think it is indicative of where they want to take this country.

We can stop it now, but if Mr. Romney is elected President, he said on day one he wants to repeal it. When he is first sworn in he will send up legislation to repeal it, and if the Senate and the House are in Republican hands, we can kiss it goodbye. It is gone. We will not be able to stop it then.

It is hard to believe, but prior to the Affordable Care Act essential services that were unique to women, such as maternity care, were not often included in health plans. Tomorrow, we include preventive care checkups, screening for gestational diabetes, and breast-feeding support and supplies.

How many low-income women in this country would know that the best thing for their babies is breast milk? Breast feeding, we know, is the preferred method of starting off babies, but sometimes these supplies can be expensive, especially if women are working at a low-wage job and they may need these supplies, but they can't afford it, so, therefore, they turn to another method, to formula for the babies. I am not saying formula is bad, but as we know, and doctors will tell us—every pediatrician will tell us that breast feeding is the best. But women would be forced to choose the less best option if they didn't have these breast-feeding supports and supplies.

Let me take head on, if I can, this idea of contraception. As the Senator from New Hampshire pointed out, this can be pretty expensive—up to $600 a year or more. For one of us who is making $172,000 a year and have great health care coverage, that is not a big deal. But to a low-income woman with a couple of kids, working at a minimum wage job, trying to scrape enough just to get by, $600 a year is a lot of money.

Let me point out another facet of this issue. Somehow people think, for example, birth control pills are only to prevent a pregnancy. There are many young women of childbearing age in this country who take birth control pills on the advice of their doctor not to avoid a pregnancy but because their monthly cycles are so painful that they can't even work. So what are we saying? A young woman who gets a prescription from the doctor and says it is not for birth control but is for other physical problems, she has to take that in and show it to her employer now or her insurance carrier? That makes women second-class citizens again. Nonsense.

I respect religious freedom as much as anyone, but despite the Republican propaganda, this law doesn't mandate that any woman has to use contraception, and it doesn't force employers to provide it. It gives women affordable access to birth control for a variety of reasons should they and their doctor decide it is right for them or their families. As for religious organizations that object to contraception, the President has issued a very sensible compromise to accommodate their beliefs, while ensuring that women still have access to this critical service.

I respect the views of all people on these often divisive issues, and I would oppose any measure that threatens the fundamental religious liberties of people or institutions. But the Republicans are not motivated by a genuine desire to protect religious liberty; rather, they are determined to undo these and other benefits for women in the Affordable Care Act. They have repeatedly introduced legislation, approved by the House Appropriations Committee, that allows anyone to opt out of providing services to which they have any religious or moral objection.

Well, one might say that sounds reasonable on the face of it, but think about this. Any employer with any religious or moral objection could opt out of any coverage. They could say, well, they object not only to contraception but to mammograms, prenatal screening. They just have a moral objection to that based upon their religious beliefs.

I respect Christian scientists—I always have—and their beliefs. Can they say, well, they are not going to cover insurance for an employee who goes to see a doctor for allopathic medical care, that is not their religious belief?

We have to have reasonable compromise, and I believe the President has come up with that. So what the Republicans would do, according to their leader, is rob 47 million women of these new preventive services. They would rob 1 million young women of the insurance they have already gained

through the Affordable Care Act, of an extension of dependent coverage. America's women will not be dragged backward. They are not going to allow health insurance companies to return to the policies and abuses that hurt them and their families prior to the passage of the Affordable Care Act.

Tomorrow marks another step forward in transforming our current sick care system into a true health care system, and many women will now experience this firsthand. We are going forward. The Republicans can bring it up time and time again. They have sent a very clear signal to the women of America that whatever they gain out of the Affordable Care Act—all these benefits—they are going to take them away from women if they put them in office.

I think the women of America need to have some deep soul searching about who they want deciding their fate in the future, after this next election.

I yield the floor.

The ACTING PRESIDENT pro tempore. The Senator from Illinois.

Mr. DURBIN. First, I thank my colleague from Iowa, Senator HARKIN, for the clarity of his statement, for his sincerity and, most importantly, for his leadership. We have the Affordable Care Act because of TOM HARKIN, Chris Dodd, BARBARA MIKULSKI, and others who worked hard to make sure it was here to help families all across America, particularly those in low-income situations.

Like Senator HARKIN, I was stunned this morning when the Republican leader came to the floor and said: The first thing we want to do is to repeal all of this health care preventive care that will be available across America, including the provisions that go into effect tomorrow protecting 47 million of our women and family members all across the United States—2 million in Illinois, I might add, will be helped by this. They insist on bringing up on the pending bill on the Senate floor this amendment to basically remove the protection for these women that is built into the Affordable Care Act.

I have to say to Senator HARKIN, we can't be too surprised at this. Does the Senator remember the very first amendment the Republicans offered on the Transportation bill—a bill that we wanted to pass to build highways and airports? Remember what Senator BLUNT, the Republican from Missouri, offered as the first Republican amendment to the Transportation bill? It was on family planning. Family planning on transportation? I guess some late night comedian can make a connection, but I don't get it.

Now we have the pending cyber security bill to protect America from a cyber attack that could cost American lives—something we are told is the No. 1 threat to America—and Senator MCCONNELL comes to the floor on behalf of the Republicans and says: This bill won't go forward unless we can offer an amendment to repeal the Affordable Care Act—repeal the protections that are there for families and women across America.

It is stunning that no matter what issue we go to the Republican Senators return to this issue of denying health care coverage and denying protection and preventive care to our families. In a way—the Senator touched on it—it is pretty easy for a Senator to come to the floor and talk about somebody else's health care because, as you and I know, and Senator MCCONNELL knows, the health care we have as Members of the Senate—American families would die for the health care we have. We have the best health care insurance in the world, and we have it in a government-administered plan that protects every Senator and their family. We are lucky. We are in the Federal Employees Health Benefits Plan. I believe people across America should have the same opportunity for the same type of health care.

I am still waiting for the first Republican Senator who gets up on the floor and denounces government-administered health care to walk to the well and say: As a proof of my sincerity, I am going to abandon my own health insurance as a Senator. Not one has done that, not a single one.

So for the Senators who come to the floor, their wives will still be protected by our health insurance, and their daughters will still be protected. The question we have to ask is, Should the protection we have as Senators for our families be available to others all across America? That is what this is about.

Tomorrow is the launch of an amazing development in health care protection for our families. I applaud it. My wife and I are still celebrating because our daughter gave birth to twins in November. We have twin grandchildren—now 8 months old. They got through the pregnancy well; she was cared for and did just great. We are so proud of our daughter, our son-in-law, and their family. I think about the provision that will go into effect tomorrow. The Senator from Iowa knows that pregnant women in danger of gestational diabetes that could threaten their lives and the lives of the babies they are carrying will have preventive screening to protect them.

Don't come to the floor and tell me you are pro-life and pro-family and you oppose that. If you want a healthy mom and baby, this screening that starts tomorrow for millions of American women is going to be a step forward, a positive step toward uneventful births and healthy babies. Think about the care and screening for cancer and for all of the problems that women face.

I see Senator MURRAY on the Senate floor. She has been an extraordinary leader on this issue. I will yield to her in a moment.

All those who are on this campaign to repeal ObamaCare—that was their slur on that, and we accept it. It was accomplished under President Obama, and I was proud to vote for it. It is one of the most important votes I ever cast as a Member of the Senate. Those who want to repeal this so-called ObamaCare—as Senator MCCONNELL called for again today on behalf of the Republicans—would repeal a few basic things we should not forget. Every family in America has a child with a preexisting condition. Think of asthma, diabetes, or a history of cancer.

Under our law, they cannot be denied health insurance coverage. We protect those kids, and we protect their families. The Senate Republicans want to repeal it. Seniors across America who are paying for prescription drugs and going into their savings to fill the doughnut hole each year are getting a helping hand from the affordable health care act. The Senate Republicans want to repeal it. Families across America with kids fresh out of college looking for jobs and can't find them or have a job without good health care can still be covered under their parents' policy until the young person reaches the age of 26. That is what the affordable health care act does. The Senate Republicans want to repeal it. And tomorrow 47 million women in America will have preventive screening so they can be healthy on an affordable basis and be mothers giving birth to healthy babies. That is in this new law, and the Senate Republicans want to repeal it.

This isn't just a war against the pill. This isn't just a war against family planning. It is literally a war against women. And the statements of the Senate Republican leader on the floor today are proof positive that they have one focus, and that is to take away these protections we built into the law.

I am happy to yield the floor for our leader on this issue, my colleague from Washington State.

The PRESIDING OFFICER (Mr. MANCHIN). The Senator from Washington.

Mrs. MURRAY. Mr. President, I come to the floor today very excited about the great progress America is going to make tomorrow, August 1, for women across this country and to share the outrage I just heard from the Senator from Illinois and others that before those even go into effect tomorrow, on the eve of this great opportunity for so many women, the Republican leader has come to the floor and said: We want to repeal it—first amendment, on an issue not related at all to cyber security but to take those away before they even begin.

It is an exciting moment for women in this country. Two years ago health insurance companies could deny women care due to so-called preexisting conditions such as pregnancy or being a victim of domestic violence—denied. Two years ago women were legally discriminated against when it came to insurance premiums and were often paying more for coverage than their male counterparts.

Two years ago women did not have access to the full range of recommended preventive care, such as mammograms or prenatal screenings, that the Senator from Illinois talked about. Two years ago insurance companies had all the leverage. Two years ago, too often, women paid the price. That is why I am so proud today to come to the floor with so many of our colleagues to highlight just how far we have come for women in the past 2 years and the new ways women will benefit from health care reform starting tomorrow, August 1.

Since the Affordable Care Act became the law of the land, women have now been treated more fairly when it comes to health care costs and options. Deductibles and other expenses have been capped, so a health care crisis won't cause a family to lose their home or their life savings. Women can use the health care exchanges to pick quality plans that work for themselves and their families. And if they change jobs or have to move, which so many people have to do today, they can keep their coverage.

Starting tomorrow, August 1, additional types of maternity care are going to be covered. Women will be armed with the proper tools and resources in order to take the right steps to have a healthy pregnancy. Starting tomorrow, women will have access to domestic partner violence screening and counseling, as well as screening for sexually transmitted infections. Starting tomorrow, women will finally have access to affordable birth control so we can lower rates in maternal and infant mortality and reduce the risk of ovarian cancer and improve overall health outcomes and encourage far fewer unintended pregnancies and abortions, which is a goal we all share.

I also wish to note that the affordable contraceptive policy we put in place preserves the rights of all Americans while also protecting the rights of millions of Americans who do use contraceptives, who believe that family planning is the right choice for them, and who don't deserve to have politics or ideology prevent them from getting the coverage they deserve and want.

Starting tomorrow, women will be fully in charge of their health care, not an insurance company. That is why I feel so strongly that we cannot go back to the way things were. While we can never stop working to make improvements, which we all know are important, we owe it to the women of America to make progress and not allow the clock to be rolled back on their health care needs.

Despite the recent Supreme Court decision upholding this law, I know some of our Republican colleagues are furiously working to undo all the gains we have made in health care reform for women and families. We heard the minority leader this morning come to the floor, and he wants to offer an amendment on the next bill that is now coming up on cybersecurity to repeal all of these important protections for women, that women are taking advantage of today, and certainly something we all should want for our families and our daughters and for the women in this country. I know they apparently think repealing the entire health care law would be a political winner for them, but the truth is that this law is a winner for women and for men and for children and for our health care system overall.

So I am proud to be out here with my colleagues today who are committed to making sure the benefits of this law do not get taken away from the women of America because politics and ideology should not matter when it comes to making sure women across America get the care they need at a cost they can afford.

Mr. President, I yield the floor.

The PRESIDING OFFICER. The Senator from Connecticut.

Mr. LIEBERMAN. Mr. President, as the Senate now turns its attention to the pending legislation that aims to enhance our Nation's cyber defenses, I would like to take a few moments to review where we are because I think the bill we now have on the floor brings us closer than ever to an agreement on a way to better defend our country, our prosperity, and our security against what is emerging as the most significant threat we face today, bigger than a conventional attack by a foreign enemy, bigger even than Islamist terrorism, a threat that is very different from anything we have faced before and so probably hard for most Americans to conceptualize but, trust me, it is here. That is why it is so important. We have come closer than ever to an agreement, but we are not there yet.

I have come to the floor to say to my colleagues that those of us who sponsor the pending legislation—Senators FEINSTEIN, ROCKEFELLER, COLLINS, and I—are eager to continue to work with our colleagues toward a broad bipartisan solution to this urgent national security threat—crisis. Obviously, to do that we have to begin processing amendments, and they have to be what the majority leader has said: germane or relevant. The majority leader has said we will have an open amendment process, and I thank him for that. No filling of the tree here. But the amendments have to be germane or relevant. We are dealing with a national security crisis unlike any we have faced before.

A broad bipartisan group of us met with the leaders of our cyber defense agencies yesterday—not political people, not partisan people—and they urgently appealed to us to pass this legislation in this session of Congress. It gives them authority to protect us that they don't have now. Frankly, they worry that without that authority to share information with the private sector, for the private sector to share cyber threat information with each other without fear of liability, for the government to have the ability to create some standards for the private owners of cyber space and then give them the voluntary option to abide by those standards—that all of those add-ons, all of those realities that will be created by passage of this bill are desperately needed now. The fact is they were needed yesterday. They were needed last year.

That is why I am so disheartened to hear this morning that our friends in the Republican caucus are talking about introducing an amendment to this bill that will repeal ObamaCare, as they call it. There is a day for that, but it is not this week on this bill. Frankly, I feel the same way about some of the gun control amendments that have been submitted by members of the Democratic caucus. Those amendments deserve debate at some point but not this week on this bill.

We can get this bill done and protect our security. Nobody believes that we are going to repeal ObamaCare this week or that we are going to adopt gun control legislation. Those are making a statement. They are sending a political message. And they will get in the way of us protecting our national security.

So I appeal to my colleagues on both sides, pull back these irrelevant amendments. Let's have a full and open debate on cyber security, and let's get it done this week. There are already more than 70 amendments filed that are germane or relevant.

The PRESIDING OFFICER. The time for the majority has expired.

Mr. LIEBERMAN. I ask my friend from Kansas if I could have 2 more minutes.

The PRESIDING OFFICER. Is there objection? Without objection, it is so ordered.

Mr. LIEBERMAN. I thank the Senator from Kansas.

There are already 70 amendments filed, so we don't have time to sit here staring at each other while we could be working through them. The truth is that we have a number of amendments on which we are ready to take votes, but of course we need cooperation from both sides in order to nail down that agreement with the consent that is required.

Before I yield the floor, I wish to underscore that while there are important issues we still need to work through this week, the reality is that because Senators on all sides have been willing to compromise, we have a golden opportunity to prove we can work together when it counts the most, which is in defense of our security and prosperity. Leading sponsors of the pending bill, leading sponsors of the leading opposition bill, SECURE IT, and leaders of the peacemakers in between led by Senators KYL and WHITEHOUSE have been meeting for the last week and making progress. And I would say that what was once a wide chasm separating us is now a narrow ridge, which we can bridge—and I firmly believe we will—with good faith on all sides, in a willingness to compromise. You can rarely get 100 percent

of what you want in a democratic—small ''d''—legislature such as ours, but if each side can get 75 or 80 percent and we can begin to fix a problem and close the vulnerabilities that exist in our cyber infrastructure this week, we will have done exactly what the American people want us to do. That is my appeal to my colleagues.

Mr. President, I thank the Chair, and I yield the floor.

The PRESIDING OFFICER. The Senator from Kansas.

Mr. ROBERTS. Mr. President, I wish to thank my distinguished friend and colleague, Senator LIEBERMAN, for his leadership and for urging Members of Congress to bring amendments down that are germane on very serious national security issues. So I again thank him for his comments and his leadership.

HONOR FLIGHT NETWORK

Mr. ROBERTS. Mr. President, I rise today to recognize a distinguished group of World War II veterans from Kansas who are now visiting their Nation's Capital this week as part of the Honor Flight Network.

The Honor Flight Network is an organization with the main mission to give veterans the opportunity to visit their memorials on the National Mall, free of cost to the veteran. The veterans who participate are many times unsung heroes of World War II, and in many cases their remembrances and their stories are shared for the first time and become public for the first time for families and hometowns. In many cases, young people traveling with these veterans hear the stories and can put the stories of these famous battles that protected our country in their local newspapers and in their school newspapers. It is history—it is history shared, lessons learned, and certainly renewed thanks to the ''greatest generation.''

Many of these veterans are in their eighties and nineties. There are fewer than 20,000 World War II veterans in Kansas. As time marches on, that number only decreases. Nationwide, the VA estimates that approximately 740 members of the ''greatest generation'' pass each day. So I am especially pleased that this Tuesday a group of 28 veterans will fly in to our Nation's Capital from Kansas to see their World War II memorial, and other memorials, and allow us the privilege to pay homage to their heroism. With five regional hubs in Kansas, there is a steady stream of veteran groups making their way to our Nation's Capital. The leaders of these groups include Brian Spencer and Bill Patterson leading the Honor Flight Kansas Student Edition from Lyndon, KS; Adrianne McDaniel and Peggy Hill, who lead the Jackson Heights Honor Flight; Beverly Mortimer and Denise Cyr head up the North Central Kansas Honor Flight out of Concordia, KS; Mike Kastle and Jeff True guide the Southern Coffey County High School Honor Flight out of Leroy, KS; and finally, the leaders of this group coming in on Tuesday are Mike VanCampen and Lowell Downey.

These hub leaders and the many volunteers deserve our recognition for the hours of work, organization, and fundraising that go into planning these trips. Thank you for what you do and for setting such a fine example in remembering and honoring the sacrifices made by those who stood in defense of our country in World War II.

Kansans and all Americans should know that this program—as a matter of fact, the World War II Memorial itself would not even exist without our former Senate majority leader, the senior Senator from Kansas and a World War II veteran himself, Bob Dole. Bob was instrumental in bringing the World War II Memorial to the National Mall. And even now Bob meets personally with Honor Flight groups who make their way out to see their memorial. When veterans learn that Bob Dole is at the World War II memorial, there is a crush of veterans like a flock of chickens going to the mother hen. I am not sure Bob Dole will appreciate that allegory, but at least I think that indicates everybody comes to hear him and thank him for his efforts.

Finally, I wish to recognize each member of this Honor Flight trip from Kansas visiting their memorial, and I ask unanimous consent that their names be printed in the CONGRESSIONAL RECORD.

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

KANSAS HONOR FLIGHT NETWORK TRIP—JULY 31–AUG. 2, 2012—WORLD WAR II AND KOREAN WAR VETERANS

WORLD WAR II VETERANS

Dwight E. Aldrich; William Henry Bernard; Eugene H. Brown; Thomas Dale Coffman; Glenn J. Compton; Richard D. Ellison; Perry L. Garten; Bob F. Holdaway; Edwin D. Jacques; Paul H. Koehn; Jay Edwin Kramer; Howard Russell Krohn; Howard Logan; Ralph Lundell; John L. Meyer; Richard Morrow Mosier; Charles G. Niemberger; Harvey L. Peck; Donald L. Revert (Don); John Russel Roberts; Rix D. Shanline; Lowell L. Smart; Norbert E. Stigge (Doc); John D. Topham; Delmar L. Yarrow; George A. Yohn; Keith R. Zinn.

KOREAN WAR VETERAN

Richard D. Wood.

I yield the floor and suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The assistant legislative clerk proceeded to call the roll.

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

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

Mr. LIEBERMAN. Mr. President, I know under the order this hour is reserved for Members of the Republican caucus, and although I am an Independent, I don't qualify exactly under the terms of the agreement to speak now. But seeing no Member of the Republican caucus on the floor, I thought I would take the opportunity to continue to speak about the pending item, S. 3414, the Cybersecurity Act of 2012, and if any of my colleagues arrive, I will yield to them immediately.

Before I yielded to Senator ROBERTS a short while ago, I made a statement that the two sides, if I can put it that way; that is, the sponsors of the pending legislation, Senators COLLINS, FEINSTEIN, ROCKEFELLER, and myself, and the sponsors of essentially the alternate approach, SECURE IT, sponsored by Senators MCCAIN, CHAMBLISS, HUTCHISON, and others—have been meeting. We have particularly been assisted by the bridge builders here—blessed are the peacemakers—Senators KYL, WHITEHOUSE, and others, and we have been making progress. I said what was once a chasm separating us is now a narrow ridge that we are close to bridging. Let me explain what I mean by that.

The sponsors of S. 3414, the pending legislation, strongly believe that owners of critical cyber infrastructure—and this is a unique aspect of our free society, thank God; 80 to 85 percent of the critical infrastructure in our country is privately owned, including cyber infrastructure. That is the way it ought to be. But it means when critical cyber infrastructure in a new world becomes a target of cyber attack and cyber theft, that we—the rest of us Americans—represented by the government, have to enter into a partnership with the private sector owners of critical cyber infrastructure so they will take steps to protect the cyber space that they own and operate because, if they don't, the whole country is in jeopardy. If an electric grid is knocked out, the kind of awful experiences we have all had at different times when the power grid has been out in our area of the country will be felt perhaps for weeks and weeks.

Think about it. What if the financial cyber system, Wall Street, the hub of the systems that handle millions—trillions, really—of transactions over and over again, were knocked out? It would have a devastating effect on our economy, let alone the most nightmarish, which is that some enemy breaks into the cyber-control system of a dam holding back water and opens the dam and floods surrounding communities with a terrible loss of life. We could go on and on with the nightmare scenarios, but they are out there, and we are vulnerable to them.

So the sponsors of S. 3414 have felt that private sector owners of critical infrastructure should be mandated—that is only the owners of the most critical infrastructure—to adopt the standards that would be set under our legislation to protect their systems and our country. Sponsors of the SECURE IT Act started this debate firmly convinced that the only thing we need to do is to enhance our cyber security information-sharing between private sector operators and between the government and the private sector. We have a section in our bill that does exactly that, but we feel that is not

enough. We feel there also needs to be these standards set for the private operators of the electric grid, of the transportation system, of the financial system, et cetera. If both sides had just stuck to their guns, no legislation would be possible. But when it comes to cyber security, no legislation, which is to say the status quo, is not only unacceptable, it is dangerous. Some of our real—really most of our national security leaders in this country from the last two administrations, the George W. Bush administration and the Barack Obama administration—have warned, as if in a single voice, that we are already facing the equivalent of a digital Pearl Harbor or a 9/11 if we don't shore up and defend our exposed cyber flanks. The same is true of the impact of our vulnerability in cyber space to cyber theft.

GEN Keith Alexander, the head of the Defense Department Cyber Command and the National Security Agency, made a speech a week or two ago in which he estimated that more than $1 trillion has been stolen over cyber space from America. He called it the largest transfer of wealth in history. That results from moving money out of bank accounts that a lot of us never hear about because the banks believe it would be embarrassing if we knew, the theft of industrial secrets to other countries that then builds from those industrial secrets and creates the jobs in their countries that our companies wanted to create here. So there is a unified position among national security leaders, apart from which administration they served under, that we need this legislation, and we need it urgently.

Several of us met with the leaders of the cyber security agencies of this administration yesterday. These are not political people; these are professionals from the Department of Homeland Security, the Department of Defense, the FBI, and others. They warned us again that the cyber systems that are privately owned and that are critical to our Nation's security remain terribly vulnerable to attack. They said to us, and I am paraphrasing, that we need this legislation to respond urgently and effectively to an attack on infrastructure as critical as the electric grid or Wall Street itself.

One of the leaders in our government, uniformed leaders, said to him today is a little bit like 1993 when it comes to cyber security; when, as we will remember, al-Qaida launched a precursor attack on the Twin Towers in New York with a truck bomb that blew up in the parking garage. We all know there was a loss of life then, but the damage was relatively small. But al-Qaida persisted and, of course, on 9/11 succeeded in bringing down the two towers of the World Trade Center. This leader of cyber security efforts in our government said our adversaries in cyber space are just about where al-Qaida was in 1993 when they blew up that truck bomb in the parking garage of the World Trade Center.

What I was impressed with yesterday, I will say parenthetically, is though there is some controversy out here about who is capable of what in our Federal Government—and let me speak frankly. Some people don't have much respect for the Department of Homeland Security. I don't understand why because they do a great job, in my opinion, in so many different areas, including the one that is relevant here, cyber security. But it was clear that the Department of Homeland Security, the Department of Defense, and the FBI are working as a team—really, like a seamless team—24/7, 365 days a year to leverage each other's capabilities to provide for the common defense. They all agreed yesterday we need to pass this legislation to give them the tools they urgently need, that they don't have without this legislation, to work with one another and the private sector.

I wish to again give thanks to Senators KYL and WHITEHOUSE, joined by Senators MIKULSKI, BLUNT, COONS, GRAHAM, COATS, and BLUMENTHAL, who have come together with a compromise proposal after a series of good-faith negotiations and, as a result, Senators COLLINS, ROCKEFELLER, FEINSTEIN, and I have made major and difficult compromises in our original bill in order to move the legislation forward, to get something started, to protect our cyber security.

I think we now have a broad agreement on a bill containing those same cyber security standards that were in our original bill that resulted from a collaborative public-private sector process and negotiation. But now, instead of mandating them, we are going to create incentives for the private sector to opt into them. We are going to use carrots instead of sticks. We have added some compromises also from the original legislation to guarantee Members of the Senate and millions of people out in the country that when we act to share information from the private sector to the government, we are going to have due regard for the privacy of people's data in cyber space—personal information—without compromising our national security at all.

There are advocates on both sides of both the information-sharing provision and the critical cyber-standards provision that think we have gone too far, and some think we haven't gone far enough. But while advocates on the outside of the Senate can hold fast to their particular positions, legislators on the inside of the Senate need to take all of these deeply held views into account. Ultimately, our responsibility is to get something done to protect our security—it is our responsibility to pass a law—and we have done that here.

I wish to first review some of the broad areas of agreement and then outline the differences that remain because I want my colleagues to understand how much progress has already been made. Sometimes the news stresses the differences between us.

Let me start with title I of the bill, which is the one on critical infrastructure. I think there is a growing, broad agreement now that the private sector owners of critical infrastructure should work with the government to develop what somebody yesterday called the best cyber hygiene or standards of defense that are needed to safeguard their facilities and the rest of us.

In the original bill we had the Department of Homeland Security playing the singular role for the government. We broaden that now in response to, particularly, recommendations from the Kyl-Whitehouse group, and we have created a new interagency council we call the national cyber security council, which will consist of the Department of Homeland Security, the Department of Defense, the Department of Commerce, the FBI, and the Director of National Intelligence, as well as relevant primary regulators when that sector of cyber structure is put forth in the council.

What do I mean by that? If they are dealing with the cyber security of the financial sector of our government, then on those standards we would expect the Securities and Exchange Commission and the Treasury Department, for instance, among others, to be seated at the table to come up with an agreement on those standards.

We have also agreed that adoption of these practices will be voluntary and that there will be no duplication of existing regulations or any new regulatory authorities that will be added to law.

We have also agreed that incentives need to be created—the carrots I spoke about, such as liability protection—to entice private sector owners to adopt these practices once they have been developed—totally voluntary. But I think if we build this right, they will come. Although it is not mandatory, we will set a standard, and private sector operators of critical infrastructure will want to meet that standard because they will want to act in the national interests to protect their customers, but also because when they do they will receive very valuable immunity from liability in the event of an attack or a theft.

Look, I decided that we needed to make the system voluntary in order to get something passed this year. I think it has a good chance of working as a voluntary system. But if it doesn't, and the cyber threat grows as much as I think it will, then some future Congress is going to come along and make it mandatory.

So there will be an incentive on both the public and private sector—particularly the private sector—to make this voluntary system work. God forbid between now and then there is a major cyber attack against our country; Congress will come flying back and adopt mandatory regulations. That is not what we want to happen. This is the time for rational, thoughtful discussion and legislation that will begin a

process that will go on for years because the cyber threat is not going away.

So that is title I. That is the compromise we offered on title I, which deals with cyber infrastructure. I go now to title VII. In between there are some very good titles, titles II through VI, but the good news is—maybe I should stress this—there seems to be broad bipartisan agreement on those titles.

Title VII is the one on information sharing, and there is some disagreement on that. But we have come to agree that private sector companies must be able to share cyber-threat information with the government and each other, with protections against liability that will incentivize—really allow—that sharing; that this sharing must be instantaneous.

In other words, to protect—to respond to concerns about private data being shared when a private sector operator of cyber security shares information with the government, we are requiring in this bill, the pending legislation, that the first point of contact for cyber sharing and reporting cyber attack is with a civilian agency—not a military or law enforcement agency or an intelligence agency but a civilian agency, such as the Department of Homeland Security or some other approved civilian exchange.

Some people have worried that if we did that, it would delay the referral of that information to the law enforcement and intelligence and military parts of our government, almost as if when the information of a cyber attack is sent to the Department of Homeland Security, somebody is going to have to go find the Secretary of Homeland Security to make sure she sees it before it goes to the Department of Defense, FBI. The world we are in is very different from that. It has been explained to me and others who met with, particularly, General Alexander, the head of Cyber Command at the Department of Defense that everything travels instantaneously, at cyber speed. That means that according to preset programs, cyber attack, if this bill is passed, will automatically—notification of it—go to the Department of Homeland Security or a civilian exchange, and at the same instant it will go to the Department of Defense, the FBI, and the intelligence community.

But when it first goes to the civilian exchange, there will be software in there to screen out—to prevent the possibility that any personal data—emails, private financial information—will not be sent to the law enforcement and defense branches of our government. That is another reason sharing will have to be instantaneous—that existing information-sharing relationships will continue undisturbed; that is, for instance, between the defense contractor and the Defense Department, and that there should be no stovepipes among government agencies. Agencies that need information should have access the instant it is provided to the government.

I know some colleagues want more assurance that while a lead civilian agency will serve as the hub for immediate distribution of cyber-threat information, it will do so without slowing down DOD's and NSA's abilities to access and act on that information. I have just told my colleagues that would be the case. Others want to add further privacy protections. I do want to say in this regard that we have already significantly strengthened the privacy protections, thanks to a lot of good negotiation with a group of Senators—Senators FRANKEN, DURBIN, COONS, WYDEN, and others—and a broad range of privacy and civil liberties groups ranging, really quite remarkably, from the left to right and in between, who seem generally pleased with what we have done to protect privacy under our legislation.

Here is the good news: The people in charge of cyber security in our government say the privacy protections we have added in the underlying bill to the information-sharing section of this bill will not stop them for a millisecond from receiving the information they need and protecting our national security. So, to me, this is the Senate at its best.

We are not there. My dream—because this is—we are legislating here. We are not in the midst of some traditional sort of government regulation controversy. We are legislating actually in the midst of a war because we are already being attacked every day over cyber space. We have been lucky that it hasn't been a major attack that has actually knocked out part of our cyber infrastructure, but that vulnerability is there.

A few months ago there was a story in the Washington Post about a young man in a country far away that launched an attack against a small utility—I believe it was a water company—in Texas. He got into their system and actually had the ability to totally disrupt the water supply in that area of Texas. What the hacker did instead—and he just had a computer and was smart—what he did instead was post proof that he had broken into the industrial control system in that small utility in Texas just to show the vulnerability. In a sense, he might have been bragging he could do it, but it also was a warning to us. What if the next time that happens it is a larger utility or a group of smaller utilities around the country—maybe water, maybe electricity, maybe gas—and this time they are not just warning us or showing us our vulnerability, but they are actually going to disrupt the flow of electricity or water to people who depend on that? That is the kind of crisis we face and why it is so urgent that we deal with this.

So let me come back to my dream. My goal here is that as we go on this week, we are able to submit a managers' amendment, but it is not just from the managers—Senators COLLINS, ROCKEFELLER, FEINSTEIN, and me—that we are joined by a much broader group and we form a broad bipartisan consensus to protect our country from a terrible danger that is real, urgent, and growing.

I always like to think back at these moments—and I was thinking about it again in this case, and since I do not see anybody else on the floor, I will indulge myself and go back—to a hot July day in Philadelphia, over 225 years ago, when the U.S. Senate was created as part of the—I am glad to say, proud to say—Connecticut Compromise offered to the Constitutional Convention by two of Connecticut's delegates to that convention, Roger Sherman and Oliver Ellsworth. It passed by just a single vote, but it helped keep the convention together and to enable our new government, including our Congress, to take shape because the Connecticut Compromise guaranteed the small States that their interests would be protected—small-population States—in the Senate because every State, no matter how big or small its population, would have two Senators, and it guaranteed the larger States that they would have a greater say in the House of Representatives, whose membership would be reflected, as it still is today, by population. Not everyone got everything they wanted that day, but they found a common ground that allowed them to go forward and finish writing our Constitution. That is the kind of position we are in today.

Shortly after the Connecticut Compromise was adopted at the Constitutional Convention, James Madison, as you know, Mr. President, often referred to as the father of the Constitution, wrote—and I am paraphrasing a little bit here—''the nature of the senatorial trust'' would allow it to proceed with ''coolness'' and ''wisdom.'' I think these negotiations on the Cybersecurity Act of 2012 show thus far that we have the ability to put ideological rigidity, partisanship, and politics aside when our security is at risk and move beyond gridlock and fulfill our Founders' vision of what this body can do when it comes to debating the great challenges of our time, with ''coolness'' and ''wisdom,'' as Madison said.

So over the next couple of days, let's debate all the relevant and germane amendments. Let's start voting as soon as we can on them. But then, for the good of the country, let's each compromise some, acknowledging that none of us can get everything we want and we cannot afford to insist on everything we want because if we do, nothing will happen and our country will remain vulnerable to cyber attack until the next opportunity Congress has—which I would guess will be sometime as next year goes on—to deal with this challenge. We cannot wait. We simply cannot wait. I know we can do this. I urge my colleagues, therefore, to come to the floor. I urge the leaders of

both parties to agree that the amendments submitted should be germane and relevant and that we can and will finish our work on this legislation this week.

I thank the Presiding Officer.

I yield the floor and suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

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

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

COTTON TRUST FUND/AGOA

Mr. MENENDEZ. Mr. President, I ask unanimous consent to enter into a colloquy with the majority leader, Senator REID, and the distinguished chairman of the Finance Committee, Senator BAUCUS.

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

Mr. MENENDEZ. Mr. President, let me begin by clearly stating I understand the majority leader later today will issue a unanimous consent request to move forward on the AGOA, the African Growth and Opportunity Act trade bill, and the Burma sanctions package as well as CAFTA–DR. Those are all efforts I supported as a member of the Finance Committee and voted for and ultimately want to see passed.

I believe trade is an effective development tool and that by investing in people we can make a long-term and sustainable change in developing countries. But at the same time, I am very concerned about our failure to reauthorize the cotton and wool trust funds which are crucial to sustaining jobs in the United States and jobs in my State of New Jersey.

For some time now I have been working tirelessly to reach an agreeable resolution on the issue, one that enables us to pass AGOA and CAFTA–DR and Burma sanctions while simultaneously protecting dwindling apparel sector jobs in the United States, hundreds in my home State, thousands across the country, and ensuring that our trade is not just free but is also fair.

That is not the case right now. So I come to the floor to enter into a colloquy with the distinguished majority leader and the chairman of the Finance Committee to ask for their help and commitment to addressing this domestic jobs issue, the cotton and wool trust funds this year, so we can seek to move this legislation and do right by American workers as we are trying to also help African workers.

I yield to the distinguished majority leader.

The PRESIDING OFFICER. The majority leader.

Mr. REID. Mr. President, I appreciate very much the Senator from New Jersey coming to the floor to discuss this issue. As my friend from New Jersey knows, as the chairman of the Finance Committee knows, I support the wool and cotton trust funds. That is very clear in the record of this body for what I believe was wrong with the Olympic uniforms. It is such a shame our athletes over there are wearing clothes made in China. I think that is too bad. I support the wool and cotton trust fund. I support the citrus trust fund. There are only three of them. I support all of them. I agree with my friend from New Jersey that we need to find a way to move these forward and ensure that American manufacturers are placed on equal footing with foreign manufacturers so there is an easier place for people to go if they want products made in the United States.

I am happy to work with Senator MENENDEZ and Chairman BAUCUS to find a vehicle to ensure that these trust funds and these American jobs are a priority that is addressed this year. So my friend has a commitment that I will do everything within my abilities to make sure we have an agreement on extending these very important trust funds this year.

The PRESIDING OFFICER. The Senator from Montana.

Mr. BAUCUS. Mr. President, I strongly endorse the suggestions made by the majority leader as well as by the Senator from New Jersey and also thank the Senator from New Jersey for pushing these measures so aggressively, the cotton trust fund and wool, and also, to some degree, the citrus which is part of this.

I support these provisions. I support the cotton trust fund, support it strongly. I am working diligently to try to find the right vehicles so we can get this passed—the cotton trust fund passed this year. I deeply appreciate the strong passion on this by Senator MENENDEZ. He has come to me many times in looking for an opportunity to pass this.

I deeply appreciate that. This place works on basic comity. Sometimes the pathways to get to a result are not well known and difficult to see, initially. But I am quite confident we are going to find a way to get this cotton trust fund passed this year. The Senator has my support to make that happen.

Mr. REID. Mr. President, before I yield to my friend from New Jersey, I wish to also state on the record that no one is a better advocate for an issue they believe in than Senator MENENDEZ from New Jersey. This is an issue he has spoken loudly and clearly about. So I reiterate what I said: I feel very compelled to do something to satisfy my friend from New Jersey on such a worthy cause.

Mr. MENENDEZ. Mr. President, I wish to thank and appreciate the majority leader's and the chairman's ongoing commitment to this issue. I look forward to continuing to work with them on the issue to protect American workers and American manufacturers from the negative effect of certain trade policies and tariffs that threaten their livelihood.

I appreciate them both coming to the floor and for their commitment. I just wish to take a minute or two for those who have asked me—I have had a whole host of our colleagues who have come and said to me: What are you trying to achieve? So we can move quickly to try to achieve the passage of AGOA and CAFTA–DR, Burma sanctions, all which I support.

I know colleagues, such as Congressman RANGEL, who was the original author of AGOA, has called, among many others. You know, very simply, pursuant to the passage of NAFTA and CAFTA and AGOA and other trade preference programs, Congress has eliminated duties on, for example, imported shirts from other countries. In some cases such as AGOA, it has also allowed the use of third-country fabrics to make those imported shirts.

Our tariff policy, however, has not changed. While foreign-made dress shirts are entering the United States duty free, we are charging American manufacturers a duty as high as 13½ percent on cotton shirting fabric. So not surprisingly, this made-in-America tax resulted in American manufacturers moving production offshore where shirting fabric is not subject to those high duties and where the finished product can come back to the United States duty free.

Six years ago, Congress recognized that, in fact, is simply unfair. Why should an American manufacturer have to pay a duty when those abroad using the same fabric can send it to the United States without any duty? They created the cotton trust fund to provide a combination of duty reductions and duty refunds to shirt manufacturers that continue manufacturing in the United States.

That program expired in 2009. Since then, these businesses have suffered and dwindled. I am just simply trying, as we promote jobs in Africa and in the Caribbean, to promote jobs in the United States. I want the women in the factories I have visited—this is the essence of how they sustain their families—to be able to continue to have those jobs.

That is why I appreciate the effort by the chairman and by the majority leader to try to get us to that point, so we can have free trade, but it also has to be fair to Americans who are here and can compete. They cannot compete when they have to pay a 13½-percent tax and people sending it from all over the world have to pay nothing. That is the essence of what I am trying to accomplish.

I will not object later today when the majority leader proposes his unanimous consent request and will support the effort to move those trade bills.

Mr. CARDIN. Would the Senator yield.

Let me thank Senator MENENDEZ for his leadership on this issue. He has been very articulate about preserving jobs and creating jobs in New Jersey and in America.

I thank him for once again standing for American workers. I thank Senator

REID, the majority leader, for his commitment to bring up the trust fund and the chairman of the Finance Committee, Senator BAUCUS, I thank him for his leadership.

Senator MENENDEZ has laid out the issue very clearly. This is an averted tariff. It works against American workers. Cotton, mainly on shirts but other commodities, such as wool and suits—as the Senator pointed out, if someone manufactures the suit or the shirt out of America and imports it into America, costing us jobs, they pay less tariff than if they are an American manufacturer that imports the product to manufacture the product in America. They pay a heavier tariff, which costs us jobs, which makes no sense whatsoever.

I thank Senator MENENDEZ for his leadership. I thank Senator REID and Senator BAUCUS for understanding this and giving us an opportunity before this expires on the wool trust fund. It is making sure it works effectively. I took the floor last week to talk about English-American Tailoring, located in Westminster, MD. There are 380 union jobs in Westminster, MD. I showed a photograph of seamstresses making suits in America. I think most people thought that photo was taken decades ago, but it was taken this month. This is about how we can preserve jobs in America. They are making the best suits in the world. They are exporting their suits to other countries, but they can't do it unless we have a level playing field.

The leadership of the Senator from New Jersey on bringing to the attention of the American people the need to extend and make effective the cotton and wool trust fund is critically important to preserving jobs in Maryland, New Jersey, and in our Nation.

Again, I thank Senator MENENDEZ, on behalf of American workers, for his leadership on this issue.

Mr. MENENDEZ. I thank my colleague.

Mr. REID. Will my friend yield to me for 1 minute?

Mr. MENENDEZ. Yes.

Mr. REID. Mr. President, I ask unanimous consent that the time for debate on S. 3414, the cyber security bill, be extended until 5 p.m. and at that time I be recognized.

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

Mr. MENENDEZ. Mr. President, I thank my distinguished colleague from Maryland, a fellow member of the Finance Committee. Senator CARDIN has been a passionate voice on this as well. I am thrilled to have him as an ally in this endeavor.

All we want is for Americans to stay employed. They can compete with anybody in the world but not when they have to pay a tariff or tax that nobody else has to pay who sends the same product back into the United States. That is our goal. I appreciate his work, his passion, and his commitment. I look forward to working with the majority leader and the chairman of the Finance Committee.

I yield the floor.

The PRESIDING OFFICER. The Senator from Connecticut.

Mr. LIEBERMAN. Mr. President, if I may have a few moments, the Senate is not in a quorum call, is it?

The PRESIDING OFFICER. There is no quorum call.

Mr. LIEBERMAN. Very briefly, Mr. President, I have just received a copy of a letter that has been sent this morning to the majority leader, Senator REID, and the Republican leader, Senator MCCONNELL, from GEN Keith Alexander of the United States Army, Director of the National Security Agency and Chief of Cyber Command at the Department of Defense. He is a distinguished and honored leader of our military, one of the people who has the greatest single responsibility for protecting our security, both in terms of the extraordinary capabilities the National Security Agency has but now increasingly for the defense of our cyber system.

This is a career military officer, not a politician. He is somebody who has a mission, and it is from that sense of responsibility that General Alexander has written to Senator REID and Senator MCCONNELL. He writes—and I will ask to have it printed in the RECORD—to express his ''strong support for passage of a comprehensive bipartisan cyber security bill by the Senate this week.'' Why? I continue to quote:

> The cyber threat facing the Nation is real and demands immediate action. The time to act is now; we simply cannot afford further delay.

He adds:

> Moreover, to be most effective in protecting against this threat to our national security, cyber security legislation should address both information sharing and core critical infrastructure hardening.

Then he explains both of those in very compelling language. He also says:

> Finally, any legislation needs to recognize that cyber security is a team sport. No single public or private entity has all of the required authorities, resources, and capabilities. Within the federal government, the Department of Defense and the Intelligence Community are now closely partnered with the Department of Homeland Security and the Federal Bureau of Investigation. The benefits of this partnership are perhaps best evidenced by the Managed Security Service (MSS) program, which affords protection to certain government components and defense companies. The legislation will help enable us to make these same protections available widely to the private sector.

I cannot thank General Alexander enough. He ends by saying this:

> The President and the Congress have rightly made cyber security a national priority. We need to move forward on comprehensive legislation now.

He urged Senators REID and MCCONNELL ''to work together to get it passed.''

I ask unanimous consent that this very compelling letter from GEN Keith Alexander be printed in the RECORD.

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

NATIONAL SECURITY AGENCY,
CENTRAL SECURITY SERVICE,
Fort George G. Meade, MD.

Hon. HARRY REID,
Majority Leader, U.S. Senate, The Capitol, Washington, DC.

DEAR SENATOR REID: I am writing to express my strong support for passage of a comprehensive bipartisan cyber security bill by the Senate this week. The cyber threat facing the Nation is real and demands immediate action. The time to act is now; we simply cannot afford further delay. Moreover, to be most effective in protecting against this threat to our national security, cyber security legislation should address both information sharing and core critical infrastructure hardening.

Both the government and the private sector have unique insights into the cyber threat facing our Nation today. Sharing these insights will enhance our mutual understanding of the threat and enable the operational collaboration that is needed to identify cyber threat indicators and mitigate them. It is important that any legislation establish a clear framework for such sharing, with robust safeguards for the privacy and civil liberties of our citizens. The American people must have confidence that threat information is being shared appropriately and in the most transparent way possible. This is why I support information to be shared through a civilian entity, with real-time, rule-based sharing of cyber security threat indicators with all relevant federal partners.

Information sharing alone, however, is insufficient to address the vulnerabilities to the Nation's core critical infrastructure. Comprehensive cyber security legislation also needs to ensure that this infrastructure is sufficiently hardened and resilient, as it is the storehouse of much of our economic prosperity. And, our national security depends on it. We face sophisticated, well-resourced adversaries who understand this. Key to addressing this peril is the adoption of minimum security requirements to harden these networks, dissuading adversaries and making it more difficult for them to conduct a successful cyber penetration. It is important that these requirements be collaboratively developed with industry and not be too burdensome. While I believe this can be done, I also believe that industry will require some form of incentives to make this happen.

Finally, any legislation needs to recognize that cyber security is a team sport. No single public or private entity has all of the required authorities, resources, and capabilities. Within the federal government, the Department of Defense and the Intelligence Community are now closely partnered with the Department of Homeland Security and the Federal Bureau of Investigation. The benefits of this partnership are perhaps best evidenced by the Managed Security Service (MSS) program, which affords protections to certain government components and defense companies. The legislation will help enable us to make these same protections available widely to the private sector.

The President and the Congress have rightly made cyber security a national priority. We need to move forward on comprehensive legislation now. I urge you to work together to get it passed.

KEITH B. ALEXANDER,
General, U.S. Army,
Director, NSA.

Mr. LIEBERMAN. 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 12:37 p.m., recessed until 2:15 p.m. and reassembled when called to order by the Presiding Officer (Mr. WEBB).

CYBERSECURITY ACT OF 2012—Continued

The PRESIDING OFFICER. The Senator from Maryland.

Ms. MIKULSKI. Mr. President, I am so glad the Presiding Officer is in the chair while I am making these remarks. I wish to salute the Presiding Officer for his service in the Senate and his service to the Nation. One knows he is a member of the U.S. Marine Corps although he no longer wears the uniform. I believe once a marine, always a marine. And his service in Vietnam and to the Nation as Secretary of the Navy is well known and well appreciated. The Presiding Officer has served as a marine in the Marine Corps and as Secretary of the Navy and now in the Senate as a Member of the Democratic Party. The Presiding Officer really serves the Nation.

I come to the floor today to talk about cyber security and the need to pass cyber security legislation this week, in this body. And I come to the floor not as a Democrat, I come to the floor as a patriot.

I say to my colleagues in the Senate that this week, on this floor, the Senate has a rendezvous with destiny. We have pending before us cyber security legislation, a framework to protect critical infrastructure of the dot-com world against cyber attacks from those who have predatory, hostile intent to the United States of America. We are bogged down. We are not moving. We are once again following what has become a usual pattern in the Senate: when all is said and done, more is going to get said than gets done.

But I say to anyone listening and anyone watching, we cannot let that happen. The United States of America is in danger. And this danger is not something in the future. It is not something written in science fiction books. This is not the wave that is going to come. It is happening right now in cyber attacks on our banking services, our personal identity, our trade secrets, and things I will talk about more.

The naysayers here say: We can't pass this bill because it will be overregulation and it will lead to strangulation, and, oh my gosh, we can't ask the private sector to spend one dime on protecting itself.

Well, I respect healthy criticism, but let me say to my friends, because I want them to know that if anything happens to the United States of America—if the grid goes down, if NASDAQ goes down, if our banking system goes down, if we will not be able to function because the streetlights won't be on and we won't be able to turn the electricity on—I will tell you what will happen. Once again, politicians will overreact, we will overregulate, and we will overspend.

In a very judicious, well-thought-out, well-discussed process, we could come up with a legislative framework that would defend the United States of America and at the same time balance that sensible center that another great patriot, Colin Powell, calls us to do: Always look for the middle ground while we look at where we want to go.

There is a cyber war, and I want everybody to know about it. Cyber attacks are happening right now. Cyber terrorists are thinking every single day about attacking our critical infrastructure. There are nation states that want to humiliate and intimidate the United States of America and cause catastrophic economic destruction. How do they want to do it? They want to take over our power grids. They want to disrupt our air traffic control. They want to disrupt the financial functioning of the United States of America. Cyber spies are working at breakneck speed to steal many of our state secrets. Cyber criminals are hacking our networks. So what are we talking about in this bill? We are talking about critical infrastructure.

Now, I am a Senator from Maryland, and the Presiding Officer is a Senator from Virginia. Does he remember that freaky storm a couple weeks ago? Remember Pepco? Oh, boy. I still have my ears ringing from my constituents calling about Pepco. I can tell you what it was like in Baltimore when that freaky storm hit. You couldn't get around when the stoplights were down. It was like the Wild West getting around. You could go into stores—if they were open—and nothing functioned. The lights weren't on. The refrigeration was off. Businesses were losing hundreds of thousands, if not millions of dollars. There were families, like a mother with an infant child and another child, with no electricity for 5 days who went to hotel rooms.

Now, they want to talk about this bill costing too much money? Just look at what it cost the national capital region of the United States of America because of a freaky storm.

It took us 5 days to get the utilities back on because of the utility company, but what happens if our destiny is outside of our control, if cyber terrorists have turned off the lights in America and we can't get them turned back on? It is going to cost too much? Wait until this kind of thing happens. I don't want it to happen, and we can prevent it from happening, and we can do it in a way that understands the needs of business.

I want to understand the needs of small business, but I sure understand the needs of families.

For those who say it is going to cost too much and they have the concerns of the chamber of commerce, fine. I don't want to trash-talk them. My father owned a little neighborhood grocery store. I know what it is like when the electricity goes down. My father lost thousands of dollars because the frozen food melted, lost thousands of dollars when we had a freaky storm because of the refrigeration and his meats and produce went bad. My father lost thousands of dollars years ago in a freaky storm.

This bill means that if we come up with the kind of legislation that we want, we can deal with it. Just remember what critical infrastructure means. It means the financial services. It means the grid. So when there is no power, schools are shut down, businesses are shut down, public transit is crippled, no traffic lights are working. By the way, in Virginia didn't 9–1-1 stop working, and they are still investigating? Don't we love to investigate? Well, right now I don't want to investigate and I don't want to castigate, but I sure want the Senate to be able to get going.

Then there is the issue of financial services. The FBI is currently investigating 400 reported cases of corporate account attacks where cyber criminals have made unauthorized transfers from bank accounts of U.S. businesses. The FBI tells me they are looking at the attempt to steal $255 million and an actual loss of $85 million. Hackers are already going into the New York Stock Exchange, they are already going into NASDAQ in an attempt to shut down or steal information. Gosh, if we allow this to continue, they could attack and cost us billions of dollars.

Does the Presiding Officer remember that in 2010 we had a flash crash? New vocabulary, new things out there. The Dow plunged 1,000 points in a matter of minutes because automatic computer traders shut down. This was the result of turbulent trading. But just imagine if terrorists or nation states that really don't like us—and I am really not going to name them, but we really know who they are—really create flash crashes?

I know there are patriots in this Senate who have been the defenders of the Nation in other wars. They have said themselves that they worry about the Asia Pacific, they worry about China. I worry about China too. So while we are looking at the Defense authorization and appropriations—and people want more aircraft carriers to defend us in the blue waters against China. But what happens if there is a cyber attack? Now, we do know how to protect dot-mil, but don't we also want to protect dot-com in the same way? I think so.

I salute Senators LIEBERMAN and COLLINS. They have come forth with a bill that does two things from a national security perspective. First of all, it tells business: You can come in voluntarily. There is no mandate to participate. But if you do come in, you will get liability protection.

Wow. In other words, we are actually going to offer incentives. We are actually going to offer good-guy bonuses. We are not going to do it through tax breaks or more things that add to the deficit or debt. We are going to say: Come on in. Participate in both the setting of standards—we want you at the table—and then living by the standards, and for that, you will get liability protection.

There are also those who say: We just don't like Department of Homeland Security being in charge. We worry about a cyber Katrina.

I worried about that too, but I must say that in all of our meetings, we can see that the Department of Homeland Security has made tremendous advances. I have been one of their sharpest critics in this area, and I have been skeptical from the beginning. But now, as we have moved along and listening to Secretary Napolitano and General Alexander, the head of the National Security Agency, on how they can work together honoring the Constitution and civil liberties, I think we have a good bill.

Why do we need this bill? General Alexander, who heads up the National Security Agency and the Cyber Command, says that we are facing attacks and the potential of attacks that are mind-boggling. He talks about the stealing of trade secrets that amounts to the greatest transfer of wealth the country has ever seen. He worries about the security of the grid. He worries about financial services, while he also worries very much about the dot-com.

But we live in the United States of America. We have a constitutional government. Our military, no matter how powerful and how strong, has a responsibility to certain areas, but we need a civilian agency in charge of how to protect dot-com, a civilian agency benefiting from the incredible turbo intellectual and technical power of the National Security Agency.

So we have a bill that offers the framework. I would say, let's have the bill, let's vote for cloture, and let's have regular order with actual germane amendments. We have patriots here, but who are we for? Are we for protecting America or are we for coming up with the same old platitudes that resist any activity of government at all to protect the American people?

I am no Janie-come-lately to this bill. I represent one of the greatest States in America. We are home to the National Security Agency. I have the high honor of being on the Intelligence Committee. I have been working on this topic for almost a decade, and I have watched the threat grow as I watched the technology against us grow in power and the number of people who could attack us in this area.

I sit on the Appropriation Committee, where, as a member of the DOD appropriations, I have been proud to work with both the authorizers and Senator INOUYE to stand up for Cyber Command, the Tenth Fleet, which is the cyber fleet, and others relating to it. But also what I have been proud of is being able to take a look at what we do need to do here in terms of everything from workforce to protecting others.

My subcommittee funds the FBI. Working with Director Mueller, I have been able to see up close and personal the growing threats right here in the United States of America, whether cyber criminals can literally invade large banking. I could give example after example. Working also with other departments, we can see that there are cyber-attacks. We need to be able to do this.

I could give other examples and I will do so in the debate, but let me summarize. The attacks are now. The question is, are we going to build a cyber bomb shelter? This is not like the bunkers of old. This is where we work with the private sector. Remember, our grid and our telecommunications are owned and operated by the private sector. We cannot do this without the private sector. We, your government, come together with a legislative framework that is constitutionally sound and legally reliable. The fact is that we will make the best and highest use of our military under that rubric. But at the end of the day we will be able to have a voluntary framework bringing the private sector together with incentives around liability that invite them to participate in the formulation of the regulation, the implementation of the regulation, and living by it. This is not regulation that leads to strangulation, this is regulation that helps them be able to protect the United States of America.

Let me conclude. Everybody says: Gee, what could I do? Could I have protected against an attack on the United States of America? What is the name of that little-known group you didn't know how to spell years ago? Al-Qaida? Would we have done everything in the world to protect against the al-Qaida attack? I certainly would. I say today, if you want to protect against the next big attacks on the United States of America, vote for cloture. Let's have an informed debate. Let's find at the end of the day the sensible center that will give us a constitutional but effective way of defending America.

I yield the floor.

I suggest the absence of quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The assistant bill clerk proceeded to call the roll.

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

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

The Senator from Wyoming.

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

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

SECOND OPINION

Mr. BARRASSO. Mr. President, I come to the floor today, as I do week after week—as a doctor who has practiced medicine in Wyoming and taken care of families in Wyoming across our State for a quarter of a century—to give a doctor's second opinion about the health care law.

One of the central claims of President Obama and Democrats in Washington who voted in this Senate Chamber was that the health care law would extend insurance coverage for millions of Americans. That was their goal. They claim that is actually what has happened. The President claimed repeatedly that 30 million more Americans would receive health coverage because of the health care law.

Well, after practicing medicine for 25 years, I understand there is a huge difference between health coverage and health care. When people have a health insurance card, then they have coverage. When people have access to a doctor, nurse, nurse practitioner, or physician's assistant, then they can receive health care.

The New York Times actually pointed that out this Sunday morning. It was the front page, above the fold. They proclaimed in the first paragraph of an article that the President's health care law delivers coverage but not care. As a matter of fact, when I take a look at this article dated Sunday, July 29, 2012, of the New York Times, page 1, above the fold, ''Doctor Shortage Likely to Worsen with Health Law,'' underneath it says that primary care is scarce, in bold letters, and beyond that it says: Expanded coverage but a greater strain on a burdened system.

The story highlights a study from the Association of American Medical Colleges, which found that in 2015, just 3 years from now, the country will face a shortage of over 60,000 doctors. By 2025, the shortage is expected to expand to approximately 130,000.

So while the Nation was already facing this shortage, the article points out it has been made worse by the President's health care law. The shortage of providers is very important because, as the article states, ''Coverage will not necessarily translate into care.'' This is especially true for those individuals who are supposed to receive their health care through Medicaid. Let's remember, a huge expansion of Medicaid was part of the President's health care law. It was part of the discussion in the Supreme Court, the decision they came out with. Of course, Medicaid is the program that provides health care for low-income Americans.

The President's health care law contained one of the largest expansions of Medicaid in the program's history. The President chose to expand the program despite the fact that fewer than half of the primary care clinicians would accept new Medicaid patients as of 2008. Fewer than half of the primary care clinicians were accepting new Medicaid

patients. Yet that is from where the President chose to build his health care reform.

Some might ask: Why is it that so many primary care physicians are not seeing Medicaid patients? It is because the reimbursements provided to doctors are so low that many can't afford to see Medicaid patients and continue to keep their doors open. Unfortunately, the outlook for Medicaid in this country has not improved.

USA Today reported in July that 13 States are moving to cut Medicaid even further by doing a couple of things. They want to reduce benefits, they want to pay health providers less, or tighten eligibility for the program. So the program the President highlights as one of the cores of his health care law is already in significant trouble, is not functioning, and is getting worse.

The State of Illinois has imposed a new limit on the number of prescription drugs that a patient who is on Medicaid can receive. This cap was imposed as part of a plan to cut $1.6 billion from the States' Medicaid Program.

Mark Heyrman, a professor at the University of Chicago Law School, told the Chicago Tribune that the prescription drug limits amount to a denial of service. So that is what we are looking at now. Yet this is the basis upon which the President has built his health care law.

According to the most recent estimate by the Congressional Budget Office, over one-third of the people expected to gain insurance coverage under the President's health care law are supposed to do it through this Medicaid Program. Clearly, with States being forced to cut back their existing Medicaid Program, there are many people who are not going to get the care they were promised through the President's health care law. For those who can find a physician, many of these patients will have to commute longer distances and will also have to endure longer waiting times just to get the treatment they are seeking.

Some experts have described this as an invisible problem, and they say that is because people may still get care, but the process of receiving that care will be more difficult.

The chief executive of the California Medical Association says, ''It results in delayed care and higher levels of acuity''—the seriousness of the injury or illness to that patient when they finally get the care they need. When care is delayed, medical problems can become much more serious, and that forces patients to seek treatment through other settings. One of the prime examples of that is heading to the emergency room.

Well, the whole goal, I remember, of the debate on the Senate floor in listening to my colleagues on the other side of the aisle was that patients under the President's health care law, the Democrats claimed, would be able to get to see a primary care doctor and would not have to go to the emergency room. However, that is not what we are finding under the President's health care law. We are finding just the opposite of what the President promised.

That is why the Medical College of Emergency Physicians told the Wall Street Journal:

> While there are provisions in the law to benefit emergency care patients, it is clear that emergency visits will increase, as we have already seen nationwide.

So the President says one thing and the American College of Emergency Physicians is telling us what they are seeing on a daily basis in emergency rooms across the country.

To put it another way, since the President's health care law exacerbated the shortage of providers, more patients are seeking treatment in emergency rooms. This is not what the American people were looking for in health reform. Instead of making empty promises, supporters of the health care law should have dealt with the issues that are already causing many doctors to rethink their medical career.

For example, supporters of the law absolutely refused to deal with the crushing burden of the medical lawsuit abuse. It is an abusive situation that is forcing doctors to practice a significant amount of defensive medicine, which is very expensive. It is expensive for individual patients as well as expensive for the system.

The Harvard School of Public Health found that these costs amount to 2.4 percent of annual health spending in the United States or $55 billion in 2008. That is the Harvard School of Public Health. There are other estimates out there which go with much higher numbers. Apparently supporters of the law thought it was more important to help trial lawyers instead of patients.

As a matter of fact, Howard Dean, chairman of the Democratic National Committee, has said they left lawsuit abuse out of the health care law because of the significant impact that trial lawyers have as contributors to the Democratic Party. So here we are.

Additionally, the health care law does nothing to stop the crushing burden of government regulations and paperwork that is consuming the health care profession.

Finally, many people choose to become doctors because they enjoy being able to innovate and create the next generation of devices and treatments. Unfortunately, that is changing as a result of the significant taxes that are part of the health care law.

In an article published on Friday, we have learned that Cook Medical, which is a medical device company in Indiana, announced that it was scrapping plans to expand because of the President's health care law. There are similar companies in States all across the country, many with large medical institutions who have a history of the best innovation in the land—and actually in the world—that are faced with these medical device taxes, not on profit but on the gross amount of money sales. The company said the 2.3-percent medical device tax contained in the law would stop the company from opening five new plants in the United States and add approximately 300 new good-paying jobs.

The Senate should also know that this Cook Medical Company produces medical devices that address women's health issues. Specifically, the company produces products related to gynecologic surgery, obstetrics, and assisted reproduction, to name a few. Therefore, the President's health care law is actually hurting the ability of Cook Medical and other companies to provide American women with access to cutting-edge medical technology. Why? Because of the device tax, which I believe—I believe we should repeal the entire law, but clearly we have introduced legislation to repeal the medical device tax. It is a bipartisan piece of legislation supported from both parties and should be passed immediately.

It seems Democrats are reluctant to look at parts of the health care law and repeal the law.

All this means medicine is becoming less of an attractive career choice for many young people across the country. As CNN stated in a headline from July 29, just 2 days ago, ''Your health care is covered, but who's going to treat you?''

The President and Washington Democrats did not seem interested in addressing this question when the health care law was passed. More effort was put into hiring IRS agents to look into whether a person had insurance than to actually see if there were doctors, nurses, nurse practitioners, physician assistants, and others to care for patients. Instead of focusing on policies that would give incentives for more people to become health care providers, they filled their law with empty promises the American people know today have not been kept.

It is time for Congress to repeal the President's health care law and replace it with real reforms that will improve the ability of patients to get the care they need from the doctor they choose at a lower cost.

That is why I come to the floor with a doctor's second opinion about a health care law which as the front page of the Sunday New York Times said: ''Doctor Shortage Likely to Worsen with Health Law.'' Primary care is scarce. Expanded coverage but a greater strain on a burdened system.

As I have been saying for a number of years on the Senate floor, coverage will not necessarily translate into care.

Thank you. I yield the floor, and I note the absence of a quorum.

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

The assistant bill 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. Without objection, it is so ordered.

Mr. DURBIN. Mr. President, the bill pending before us is the Cybersecurity Act of 2012, as it is known, and for most people it is a term which they may have heard but may not fully understand.

It was about 2 months ago that Members of the Senate, including the Presiding Officer, were invited to a classified briefing. It was a briefing that Senator MIKULSKI of Maryland asked for to explain what this was all about because we had been hearing over and over again from the defense establishment in America that the No. 1 threat to America's safety and security was no longer just terrorism; it was cyber security threats and terrorism. For most people, they are not quite sure they have seen any examples of it that could make a difference.

So here is what we saw. They took us down to this classified room, closed the door, took away our BlackBerries and iPhones, and put them in a separate place—and I will explain why they did that in a moment—they took us in the room and briefed us on an example, just a theory. What if? What if a subcontracting company that supplied a major public utility in a city such as New York had a problem and someone stole a laptop from one of the employees, and that theft went unnoticed or unreported for a number of days, and then the laptop either reappeared or did not, what could happen?

Well, what could happen was, if that laptop computer had certain information in it that not only told you how to get into the computer system of the subcontracting company but also the public utility, bad things could occur. So getting inside that computer laptop, getting inside the technology of the subcontractor, and then finding that information bridge into the public utility could create an opportunity to turn out the lights in the city of New York.

That was the exercise we went through. God forbid it would ever occur, but they said: When you turn out the lights in a major American city such as New York, terrible things happen. Not only do traffic signals stop, and lights do not go on at night, and the New York Stock Exchange is not operating, hospitals are on emergency generators and problems start popping up in every single direction—water purification; the pumps that keep the subway system under the city of New York going so that the subway tunnels are not flooded—all of these things on top of one another. While this tragedy is occurring, the people in our government are trying to figure out: What happened? And how do we put things back into place and get them moving again?

That was one example.

There was another example. It was an example at one of our defense research laboratories. Top secret. Nobody can get in. Right? They told us of an example—and I will not even tell you the State where it was located—they told us of an example where the employees at our top defense research laboratory—who were trying to figure out countermeasures to stop attacks against the United States, and to develop our own weaponry—had what appeared to be a harmless e-mail sent to the employees saying: Explanation of Your New Health Care Benefits. Just Click Below. It turned out that click brought the hackers into the system.

So what we are talking about here has consequences that go far beyond the harassment of some teenage hacker who is trying to get into some company computer or even the school's computer.

I was on a plane yesterday with a gentleman who is working for the National Institutes of Health. I asked him about cyber security.

He said: We think about it every day—every day—because hackers are trying to get into the National Institutes of Health technology and computer system.

I said: What for?

He said: Well, some of them are in there for insidious reasons. But some of them are childish hackers.

I said: What do they do?

He said: Well, they will come in, for example, and change our published list of antidotes to certain poisons, so we always have to keep an eye on it to make sure they have not changed what people, doctors, should use across America.

Think about it. Think about all of the possibilities. What we are trying to do today is to come up with a line of defense for America. We are trying to establish a working relationship between all levels of our government and the private sector of the United States to keep us safe. Because what they told us was, every single day, China, Russia, Iran are on the attack—cyber security attacks into the United States—not just the ones I have mentioned but far beyond. Defense contractors building the planes and the armaments and all the artillery and the like have to worry about whether their secret plans, their patented information is being stolen right from under them, stolen by someone who wants to compete with them or perhaps wants to go to war with them. That is what is at stake.

So for a long time we have been warned and forewarned to do something about it. The bipartisan consensus among defense and intelligence experts in the public and private sector is that our Nation is dangerously vulnerable to cyber-attack at this moment.

FBI Director Bob Mueller—an extraordinarily great public servant—says the threat our Nation faces from a cyber-attack will soon equal or surpass the threat from al-Qaida and more traditional forms of terrorism.

Navy ADM Mike Mullen, Chairman of the Joint Chiefs, said: ''The cyber threat has no boundaries or rules, and the reality is that cyber attacks can bring us to our knees.'' According to our Director of National Intelligence, James Clapper, countries such as Russia and China are already exploiting our vulnerability. His unclassified assessment—what he told the public—is that entities within these countries are already ''responsible for extensive illicit intrusions into U.S. computer networks and theft of intellectual property.''

We have to respond to this. We have to do it quickly. I wish to thank Senators LIEBERMAN, COLLINS, FEINSTEIN, and ROCKEFELLER for putting together this bill, the Cybersecurity Act of 2012. They have introduced an approach that is balanced, bipartisan, and responsive to legitimate concerns raised by the intelligence community, private industry, and privacy advocates. The Cybersecurity Act of 2012 will help make us safer.

Our Nation's critical infrastructure—powerplants, pipelines, electrical grids, water treatment facilities, transportation systems, even financial networks—are increasingly vulnerable to attack. Bad actors in other countries have already demonstrated their ability to use the Internet to take control of computer systems.

Last year, there was a 400-percent increase in cyber attacks on the owners of critical infrastructure. This act has provisions that will reduce our vulnerability and shore up our defenses. In response to concerns raised by some in the private sector and some on the other side of the aisle, Senators LIEBERMAN and COLLINS revised a section of the bill. The bill now creates a voluntary, incentive-based system of performance standards. Private companies and government agencies will work together to determine the best practices in each sector to prevent a cyber attack. Companies that voluntarily implement those standards will be rewarded with immunity from punitive damages in a lawsuit, receipt of real-time cyber threat information, and expedited security clearances, among other things.

This voluntary arrangement replaces the mandatory system in an early version of the bill. Many of us supported that approach. But in the spirit of compromise and responding to concerns expressed by the business community, the managers have included this voluntary approach. The Cybersecurity Act of 2012 also authorizes voluntary information sharing. The sharing provision will allow government agencies and willing private companies to enhance the mutual understanding of the real threat and our vulnerabilities.

Sharing this information on effective responses and recent cyber threats will enable both the government and the private sector to understand the threat and to respond. A handful of industries have already adopted this approach, and it significantly enhances their ability to identify and respond to cyber threats. We should empower the government to share its knowledge with

these and other industries. We should make it clear the private companies can share cyber threat indicators with the government. That is exactly what this Act does.

I wish to thank the Presiding Officer, Senator FRANKEN of Minnesota, as well as Senators COONS, BLUMENTHAL, SANDERS, and AKAKA for working with me and the managers to ensure that we protect privacy and civil liberties. The Presiding Officer is chair of the Privacy Subcommittee of the Judiciary Committee. He has been a real leader on these issues. I was happy to work with him. As a result of his efforts and our efforts, the willingness of Senators LIEBERMAN, COLLINS, ROCKEFELLER, and FEINSTEIN, we were able to significantly enhance the privacy and civil liberties protections in the revised bill. I believe—I have always believed and I will continue to believe—we can keep America safe and free. We can establish in our democratic society the appropriate defense to any threat without sacrificing our fundamental constitutional rights.

The revised bill, after we negotiated with them, now requires that the government cyber security exchanges be operated by civilian agencies within the Federal Government. Our thinking was that these agencies are more prone to oversight, and any excesses by them will be caught earlier than if this is done on the military side, to be very blunt.

Military and spy agencies should not be the first recipients of personal communications such as e-mails. But from time to time, they will need to be informed and we need to rely on their expertise. That is why the bill requires that relevant cyber threat information be shared with these agencies as appropriate in real time.

The revised bill eliminates immunities for companies that violate the privacy rights of Americans in a knowing, intentional or grossly negligent manner. To ensure that cyber security exchanges are not used to circumvent the fourth amendment, the bill requires law enforcement to only use information from the cyber exchanges to stop cyber crimes, prevent imminent death or bodily harm to adults or prevent exploitation of minors.

The revised bill creates a vigorous structure for strong, recurring, and independent oversight to guarantee transparency and accountability. It gives individuals authority to sue the government for privacy violations, to ensure compliance with the rules for protecting private information. These commonsense reforms improve the information-sharing section of the bill, and they protect privacy. That is why they have been widely embraced across the political spectrum from left to right. I think we have found the sweet spot. I think we have found the right balance. That kind of endorsement across the political spectrum suggests that is the case.

We are very vulnerable in the United States at this very moment. Our critical infrastructure is at risk, and billions of dollars' worth of intellectual property is being stolen. Our national security is compromised. To put the cyber threat in perspective, GEN Keith Alexander, Director of the National Security Agency, was asked: How prepared is the United States for a cyber attack on a scale of 1 to 10, with 10 meaning we are the most prepared. What was his answer? Three—three out of ten. That is an alarming assessment. It is a failing grade by any standard.

If we do not act now, we will continue to be at risk for not only the loss of information and economic loss but even worse, mass casualties, a crippled economy, the compromise of sensitive data. I know this bill has some controversy associated with it. I know there are some in the business sector who think we have gone too far. I would plead with them, work with us. Let us do this and do it now. To let this wait is to jeopardize the security of this country. We did not think twice to respond quickly after the 9/11 attacks to make America safe. We see it everywhere we turn. If one can even imagine what life was like in the United States before 9/11, before we took our shoes off when we went to the airport, before searches were commonplace in American life, before armed guards stood outside the U.S. Capitol—those are the realities of what we face today because of that attack.

Let's be thoughtful. Let's be careful. Let's come together, the private and public sector. Let's do this the right way to keep America safe. The people who sent us to represent them expect no less.

FOR-PROFIT COLLEGES

Mr. President, the Senate HELP Committee released a report after completing a 2-year investigation of for-profit colleges. The 1,096-page report is the most comprehensive analysis yet. It provides a broad picture of the for-profit college industry. What Senator TOM HARKIN and the committee discovered and carefully documented is an industry driven by profit, which too often has limited concern for the students or the actual learning process.

The report profiles 30 of the biggest for-profit colleges, virtually from every State in the Union, including Illinois. There are good schools there, make no mistake, and my colleague Senator HARKIN has been careful to point them out. But there are also some that are not making an effort. Some are trying to improve student outcomes. But unfortunately there are many of these for-profit schools that are just taking in, soaking in Federal subsidies in the form of student aid so they can pay their shareholders extra money.

DeVry is the third largest for-profit college in the country. It is based in my State of Illinois. DeVry operates 96 campuses and offers classes online. In 2010, DeVry had over 100,000 students, an increase of 250 percent of enrollment in 10 years since the year 2000. It derives almost 80 percent of its revenue from the Federal Government.

Similar to the other companies profiled in the report, DeVry's tuition is significantly higher than that of public colleges. The cost of tuition for a bachelor of science in business administration at DeVry's Chicago campus is $84,320—for a bachelor's degree—considerably more than the same program at the University of Illinois, where the 4-year tuition is $75,000.

DeVry looks good compared to many of its peers in the for-profit sector. Unlike some other schools, DeVry's internal documents reveal the school has chosen not to use aggressive price increases in the future. I salute them for that. I have spoken to their leadership and told them that if they want to distance themselves from the pack of bad for-profit schools, they have do it by making decisions and implementing them to demonstrate they are a different kind of for-profit school.

There are still areas where DeVry can make improvements. DeVry's institutional loan program, a private loan program, charges a 12-percent interest rate—12 percent. The Federal Government student loan, 3.4 percent in contrast. So this rate is roughly three times the Federal loan.

The HELP Committee estimates that in 2009, when all sources of Federal funds, including military and veteran's benefits are included, the 15 largest publicly traded for-profit education companies received 86 percent of their revenue from taxpayers—86 percent. They are 14 percent away from being totally Federal agencies.

Perhaps this would be acceptable if students were learning and gaining skills to succeed, but what the committee found is troubling. One of the main reasons student outcomes are so poor at these schools is that the schools do not provide students with basic support services that they need to find a job and succeed. Student support services are essential to helping students adapt and do well while they are in school and find a job. What happens instead? They drop out or, if they graduate, they cannot find a job.

In 2010, the 30 for-profit colleges examined employed 35,000-plus recruiters—35,000 recruiters. The same schools collectively employed 3,500 career service staff and 12,452 support staff. So by a margin of 2½ to 1, the schools had more recruiters than support service employees.

So we cannot be shocked when we learn that one-half million students who enrolled in 2008–2009 left without a degree or certificate by mid-2010. Among 2-year associate degree holders, almost two-thirds of the students in these for-profit schools departed without a degree, just a debt.

The report also highlighted a growing problem among for-profit colleges, the use of lead generators. For-profit colleges gathered contact information on perspective students or leads, as they call them, by paying third-party companies known as lead generators.

These generators specialize in gathering and selling information—in this case, very personal information.

Here is how it works. A student browsing the Internet searches for terms such as ''GI bill,'' ''student loan,'' ''Federal student aid'' or any variation. They are directed to various Web sites that are owned by these lead generator companies. The Web site then claims to pass the prospective student contact into an appropriate school for the student online. Typically, there is no disclosure to the student that their personal information is being sold to for-profit colleges.

When a perspective student does give their contact information, watch out. They will be bombarded with calls and e-mails from aggressive recruiters at these for-profit schools. Remember that 35,202 people are employed as recruiters. This is what they do. One of the Web sites, gibill.com, was owned by a company called QuinStreet until last month, when 23 attorneys general across the United States did what Congress should have done first. As part of an agreement, QuinStreet gave up its right to the Web site to the Veterans' Administration where it belongs. So gibill.com is no longer a deceptive Web site, at least in these 23 States where there has been an agreement. Other Web sites used the name of Federal student aid programs and misled students into believing this was a real government program.

One of the HELP Committee's recommendations is to further regulate the private student line market. Senator HARKIN and I introduced the Know Before You Owe Private Student Loan Act this year. Our bill requires private student loan lenders to verify the prospective borrower's cost of attendance with the school before disbursing the loan.

It also requires the schools to counsel students as to whether they are still eligible for Federal student loans at a much lower interest rate. Federal student loans have flexible payment plans, consumer protections, and as I said, less cost. But many times students who have not exhausted their Federal student loan aid are steered into private loans with interest rates three and four times higher. There is money to be made off those young and sometimes uninformed students.

I urge the private lenders and the for-profit schools that keep telling me ''we are doing the right thing,'' do not wait for this law. Do it now. Make this a policy at their school and prove it.

One of the students I wanted to mention is Mirella Tovar from Blue Island, IL. She graduated from Columbia College in 2010 with a B.A. in graphic design and with $90,000 in debt and with a 10.25-percent interest rate. Her balance started to grow. She did not take out any Federal loans. She thought all the loans were the same. She did not know the difference.

No one told her about the consumer protections in the Federal loans. After she used her 6-month forbearance permitted by her lender, Mirella was expected to pay $1,500 a month. Unable to get a full-time job in her field, she thought about filing for bankruptcy.

It would not have done any good; student loans are not dischargeable in bankruptcy even if they come from for-profit colleges. Her dad wanted to help, so he cosigned her private student loans. Guess what. He is now on the hook for the payments too.

Mirella says that if the school counselor would have told her more about what her monthly payment would be like, she would not have taken out so much, and she may have never been steered to a private student loan.

I thank Senator HARKIN for his leadership and his amazing work on this issue. I plead with my colleagues, on behalf of these students and their families and on behalf of the taxpayers who are subsidizing these schools, join us in setting standards so there is an opportunity for young people to get the education they need without inheriting the debts that can drag them down for a lifetime.

I yield the floor.

The PRESIDING OFFICER. The Senator from Georgia.

Mr. ISAKSON. Mr. President, I ask unanimous consent to address the Senate as in morning business.

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

REMEMBERING R. TIMOTHY STACK

Mr. ISAKSON. Mr. President, this morning I got some very sad news. The State of Georgia and the people of my State lost a giant in the health care industry.

Tim Stack was my friend. He was the president of the hospital that 2 years ago treated me well, which is why I am here today. He was a giant in health care not just in Georgia but in America. On behalf of myself and all the citizens of my State and the countless thousands of patients whose lives have been made better or even saved by Tim Stack, I send my condolences to his wife Mary and his three sons: Ryan, Tim, and Matthew.

Tim Stack grew up in Pittsburgh, PA, working in the steel mills. When the mills closed, he looked to find a job, and he worked in central supply at the Eye & Ear Hospital of Pittsburgh, PA. He was working and studying to be a teacher and a football coach. By working in the hospital, he became fascinated with the complexity of hospital administration and was challenged by the love of caring for people who were ill. Tim Stack changed his major to hospital administration and became a leader in the United States in the administration of hospitals.

Let me read from a press release on his record in Atlanta, GA, alone:

> Under his leadership, Piedmont grew from two hospitals and eight physician practices to a $1.6 billion organization that includes five hospitals, more than 50 primary care and specialty physician practices and a 900-member clinically integrated network.

He also helped develop the Piedmont Heart Institute, which treated me 2 years ago and is the reason I am standing here today, which is the leading heart institute not just in Atlanta and in Georgia but throughout the United States.

Tim was one of a kind. His loss will be felt by countless thousands of Georgians. To his family, his friends, and all who knew him, I express my sympathy.

I want to read a quote from him that was written in 2006 when he was interviewed by Atlanta Hospital News for a profile. Tim wrote the following:

> The attributes of a good leader are universal. You need to love what you do, be open and inquisitive and persistent, not afraid to make waves if you have to. You should also be personally productive and work well with others. Be innovative and allow others to innovate. Finally, be a certifiable member of the human race. Cultivate a light touch, be passionate about your career, but be sure to balance it with the rest of your life.

That expresses better than I can what Tim was all about. I shall miss him greatly, as will all of my State. Again, I send my sympathy to his wife Mary and his three sons: Tim, Ryan, and Matthew.

I yield the floor.

The PRESIDING OFFICER. The Senator from Delaware is recognized.

Mr. COONS. Mr. President, I rise to speak to the issue of cyber security, one where there have been a dozen speeches given earlier today, and one where I am concerned that there is not enough determination, not enough will on the part of this body to work together, to listen to each other, to cross the small differences that remain between camps and competing theories of a bill that we should take up, and I am here to urge our colleagues in this body to address what we have been told is one of the greatest security threats facing our country, to bear down, to file amendments, to clear amendments, to listen to other Members and be willing to do the job for which we were hired, which is to pass tough, broad, bipartisan legislation to protect this country we love.

In my short 20 months in the Senate, I have increasingly become more and more persuaded that we face a constant, steadily rising, increasingly dangerous threat that foreign nations, foreign actors, whether they be terrorists or enemies of the United States, are not just studying the possibility of some day attacking the critical infrastructure of the United States, they are not just writing position papers or theorizing about it or training in some camp in an obscure country, they are today actively engaged in thousands of efforts to compromise the critical infrastructure of this country.

How Members of this body can ignore the importance of this threat when the majority leader and the Republican leader have twice, in my short time here, closed the Senate and urged every one of us to go to a secure, classified

briefing, where we have heard from a dozen four-star generals and leaders of three-letter agencies who have told us in great detail about how grave this threat is. Why in the face of repeated and publicly cited assertions by Secretaries of Defense, heads of the NSA, leaders of our homeland security agency, and leaders responsible for our first responder community from the Federal, State, and local levels, from the private sector to this government, who have said over and over that this is a very real, very present threat—how we can ignore that threat today is beyond me.

The bill that is before us is S. 3414. This is a compromise bill. In a series of meetings with other Members of this body, I have been struck to hear others say that we need more time, we need to study this further, we need to pass the narrow portions on information sharing that are easy and everybody can now agree on, and we need not pass a broader or stronger bipartisan bill that deals with infrastructure.

As you know well, Mr. President, for years critical committees in this body have been working on this issue. Senators LIEBERMAN and COLLINS, the chair and the ranking member on Homeland Security and Governmental Affairs, have been engaged in working their way through difficult issues for years. The relevant committees, from Energy to Commerce to Intelligence, have been engaged in hearings and studies and in legislating for years before I became a Senator.

In the last few months there has been some important and strong work to build a bipartisan consensus around the bill that is before us today. I, like you, I believe, Mr. President, had some real concerns about the information-sharing portions of the bill, title VII, which have to do with permitting private companies to share information with each other about the threats of attacks.

One of our big problems right now, we are told, is that companies of all different sectors of our economy hesitate to share publicly or to share with our national security infrastructure information that is critical to knowing when we are being attacked, how we are being attacked, and how it might spread. Title VII of the bill gives them liability protection to encourage the broad and regular sharing of that information.

But those of us who are concerned about the balance between privacy and security, about protecting civil liberties and whether we have gone too far in seeking security at the expense of liberty, offered a whole series of revisions and changes to this bill—changes that have been accepted. So too in a different section of the bill—title I, which deals with critical infrastructure—folks from the private sector raised alarms and concerns months ago that this bill was too prescriptive, too heavyhanded, was involved too much in regulation and in demanding certain actions by the private sector. Those concerns, too, have been addressed in a broad way.

I have been impressed with how many changes Senators LIEBERMAN and COLLINS have been willing to accept out of a broad working group of more than a dozen Senators of both parties who over the last few months have come forward with suggestions that have made that portion of the bill truly voluntary for the private sector, in a way that balances the role of civilian agencies with parts of our national security apparatus, in a way that provides enough liability protection but not too much, and in a way that allows the private sector to have a leading role in setting standards.

My point, then, is to say to my colleagues that when they say we need more time to study it, I say we need to come to this bill, we need to come to the floor, and we need our colleagues to be clear—what are your remaining concerns? In a meeting last Friday with several Senators and representatives of industry, I had read every word of title VII and urged them to be concrete with us about what their concerns were. I left unsatisfied. I left concerned that some were simply scaring the private sector and scaring our citizens into thinking this bill is not ready.

So for those who still have concerns—and there may very well be broad and legitimate concerns about the bill and about its direction—let's take these 2 days. I understand that more than 90 amendments have been filed. I think it is the challenge before us to make the amendments germane, narrowly focused, and relevant to improve the bill rather than distracting us into issues that are more partisan or tied to the campaign and to focus on the work that is left before us.

If I could, I am gravely concerned about those who would urge us to split off the portion of the bill on information sharing and ignore the portion of the bill that has to do with protecting our critical infrastructure. As speaker after speaker has come to the floor today and made clear, our electricity grid is at risk, our dams and our powerplants are at risk, our highways and financial system are at risk. There are all sorts of areas in the United States where there have been real cyber attacks, online attacks, in other countries that have demonstrated the devastating potential power of our opponents and enemies around the world.

In the face of the cautionary notes we have heard from leaders of this body and around the country and in the face of that very strong reality, why we wouldn't pass a broad and tough bill that facilitates information sharing and protects our critical infrastructure and strikes a fair balance in the middle is beyond me. It is not that this body has been too busy. It is not that we are exhausted by having passed too many broad and strong, bipartisan bills. We have gotten good work done this session. There are things, from the farm bill to the Transportation bill, where this body has shown an ability to listen to each other across the differences of party and region and craft strong, balanced, bipartisan bills. It is on this topic of cyber security that we have heard over and over that there is no more pressing challenge.

Why, if our adversaries are not going to be taking the month of August off, if our adversaries are not going to cease from now until November to attack us, would we not bear down and focus on getting done the work that is before us as the U.S. Senate? We are called at times the world's greatest deliberative body. I will say to you as a member of the Foreign Relations Committee, in other parts of the world there are folks who are striving toward democracy who question whether this is the model they should follow.

In the remaining days before we all go to some recess, why not bear down, do our homework, do our reading, be forthcoming with clear and concise concerns, and hammer out our differences?

I extend an invitation to any colleague, any industry group, or any group of concerned citizens: I am happy to meet with anybody to hear their concerns and try to do my level best to convey them to the bill managers and the leaders, who have done a remarkable job of hearing and accepting compromise provisions of this bill on privacy, on the role of the private sector, on making voluntary what was mandatory and striking a fair balance.

I urge our colleagues to take this moment seriously, to not allow the days to slip, the month to pass, and the moment to pass us by. How will we answer our constituents, our communities, and our families following an attack that has been so frequently predicted? Do we not believe we will end up regulating in a more heavyhanded, more reactionary, and more ill-informed way after a successful massive attack than now when we have the time to listen to each other and craft a balanced and responsible and bipartisan bill?

Mr. President, I will close. I am convinced that this is the gravest threat facing our country today, graver than that of terrorism from overseas. In fact, GEN Keith Alexander of the NSA has clarified just in the last few days to a group of us how grave a threat this is.

I renew my offer to any Member of this Chamber: Come and meet with me. Come and meet with Senators LIEBERMAN and COLLINS. Come and meet with the leaders of the relevant committees, take up your cause, and give an amendment that is narrow and focused and relevant, and let us hammer out a better defense for this Nation.

There are those who question the purpose and purposefulness of this body. It has no greater purpose than finding a bipartisan way to craft a strong and vibrant solution to a clear and growing national threat.

Just a few weeks ago, I had the honor of sitting for lunch with Senator DANIEL INOUYE. He is the one Member of this body to have earned the Congressional Medal of Honor in combat. I asked his advice, as the most senior member of my party: What issues, Senator INOUYE, do you think I should be focused on? What is the thing you might urge me—a freshman—to invest my time and effort into? His answer was simple, his answer was profound, and his answer, I hope, will be heard by this body.

He said to me: I am the only Senator who was at Pearl Harbor. Our next Pearl Harbor will come from a cyber attack for which we are today unprepared. Let's do our duty. Let's listen to each other, come together, hammer out a strong and bipartisan bill, and honor the service and sacrifice of that ''greatest generation''—both in this Chamber and our country—and do our duty.

Madam President, I yield the floor.

The PRESIDING OFFICER (Mrs. SHAHEEN). The Senator from Colorado.

Mr. UDALL of Colorado. Madam President, I want to acknowledge the powerful and eloquent words of my colleague from Delaware. I know our colleague Senator COLLINS is also on the Senate floor, and I have to tell the viewers and all of my colleagues I couldn't agree more. The time is now to act on cyber security.

I just came to the floor from an Intelligence Committee briefing. General Alexander was there. As the Senator from Delaware knows, he is forthright, he is well-versed, he is passionate, and he is as nonpartisan as they come. General Alexander is urging us to act now.

So I thank my colleague from Delaware for his compelling and important words.

PRODUCTION TAX CREDIT

The matter that brought me to the floor has a link to cyber security, and that is energy security. I want to talk about one of the new and exciting technologies that is resulting in the production of many homegrown electrons, and that is wind power.

I have come to the floor on a daily basis to urge my colleagues to work with me to extend the production tax credit for wind.

The PTC has created literally tens of thousands of jobs across our country and has the potential to create even more. But if Congress—that is us, the Senate and the House—doesn't act to extend it, tens of thousands of jobs, literally, will be lost. The Presiding Officer has a robust wind energy sector in her State, and she knows the extent to which it is important for business in the great State of New Hampshire. It is important to the businesses in every State in our country.

The production tax credit is an investment in a clean energy future. It is a critical investment in American jobs. Frankly, we are about to lose that investment. I fear, in fact, that through our inaction we continue to create real harm to our wind industry in America. But it is not too late to act.

Today I am going to focus my remarks on Idaho, a State that is known for its wide open spaces, its mountains, its potatoes, and for great, friendly people. One doesn't have to look any further than Senator CRAPO and Senator RISCH to know that the people of Idaho are very good people.

Idaho is a State with a vast untapped potential for wind energy. The National Renewable Energy Laboratory, which we host in Colorado, has calculated that Idaho's wind resources could potentially provide more than 218 percent of Idaho's electricity needs. It ranks 23rd in our Nation's wind resource potential. Most of this potential is in the high plains of the southern half of the State.

Idaho is already working to take advantage of what is a bountiful resource. There are more than 20 separate wind projects either online or under construction across the State. In southeastern Idaho near Twin Falls, Invenergy's Wolverine Creek wind farm covers about 5,000 acres and pays royalties to almost 30 different landowners.

In 2011, Idaho's installed wind capacity grew by nearly 75 percent. That growth created hundreds of temporary construction jobs as well as permanent jobs in the operation and maintenance of these facilities. Right now, Idaho's wind resources provide power for nearly 160,000 homes without releasing the nearly 1.1 million metric tons of carbon dioxide that traditional power sources would.

Wind supports close to 500 jobs in the State of Idaho—jobs that wouldn't exist if the wind industry had not been enticed to invest in Idaho because of the production tax credit, the PTC. Wind energy projects are an investment in local and State economies. Wind energy producers provide nearly $2.5 million to the State in property tax payments every year and over $2 million annually in land lease payments to local Idahoans who go on to invest that money back into their local communities. Those are real dollars these communities count on.

The point I am trying to make is that we in Congress should be working to help create more projects like Wolverine Creek for the jobs and the clean energy they create. Instead, Congress is standing idly by.

I can't help but mention there have been some on the campaign trail who have suggested that we should let the wind production tax credit lapse at the end of this year, and that wind power should not be given the same help other industries have received. I could not disagree more.

Great States such as Idaho, Colorado, and New Hampshire make things. Great countries such as the United States generate their own energy. Letting the wind production tax credit lapse would be irresponsible. The PTC equals jobs. We should pass it as soon as possible. We should not waiver, and we should not wait. Every day that we let this unanswered question hang over our country may be another project and another job that gets shipped overseas.

I urge my colleagues to work with me to support manufacturing in rural communities in America. Let's extend the production tax credit as soon as possible. It is common sense. It has bipartisan support. Let's extend the production tax credit.

I will be back tomorrow to continue this discussion and talk about another one of our great States. I am at 13 States. I am going to keep coming back until we get this right.

Madam President, I yield the floor.

The PRESIDING OFFICER. The Senator from Minnesota.

Mr. FRANKEN. Madam President, I ask unanimous consent to speak as if in morning business.

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

MEDICAL LOSS RATIO

Mr. FRANKEN. Madam President, over the last few weeks hundreds of thousands of Minnesotans have received letters or postcards in the mail from their health care insurers. These notices are letting people know whether their insurer met a new rule in the health care law—a rule that I championed—called the medical loss ratio, sometimes called the 80–20 rule. It could also be called the 85–15 rule, but it is known as the 80–20 rule, and I will explain.

This provision, which I based on a Minnesota State law, requires large group insurers to spend 85 percent of the premiums they receive from their beneficiaries on actual health care services, not on marketing or administrative costs or CEO salaries. Eighty-five percent of their premium dollars have to be spent on actual health care. For insurers in a small group and individual markets, this threshold is 80 percent; hence, the 80–20 rule.

This summer, across the country Americans are getting notices from their insurers that the insurer met or did not meet this 80 or 85 percent threshold. When those notices say the insurer failed to meet the medical loss ratio, Americans are also getting something else in the mail—a check or lower premiums for next year because under my medical loss ratio provision, insurers who do not spend at least the 80 or 85 percent of premiums on actual health care services for their beneficiaries have to rebate that money to their consumers.

August 1 was the deadline for insurers who didn't meet the MLR threshold to rebate the difference to their consumers, and because of the medical loss ratio more than 123,000 Minnesotans got rebates from their insurer. Those rebates added up to an average of $160 per household. It was more in other States.

This isn't unique to Minnesota. Across the country 12.8 million Americans got rebates from their insurers who overcharged them, and other insurers lowered their premiums for last

year to comply with the medical loss ratio. Aetna in Connecticut lowered premiums by 10 percent last year because of the MLR.

Minnesota has a culture of high-quality low-cost care. In fact, the Agency for Health Care Research and Quality recently announced that in 2011, Minnesota's health care quality was the highest in the Nation. We were again No. 1. We are always No. 1, No. 2, or No. 3. The medical loss ratio, which was first passed as a Minnesota State law, is yet another example of Minnesota's leadership in bringing down health care costs while preserving quality.

Minnesota's unique health care culture includes the Mayo Clinic, cooperative models such as HealthPartners, and visionary public health leadership from State legislators. Health care in our State is also distinguished by the fact that 90 percent of Minnesotans are served by a nonprofit health plan. These plans outperform their national peers and are able to put 91 percent of every premium dollar toward actual health services. In other words, they have a 91 MLR.

By taking profits out of the health insurance industry, Minnesota health plans do a better job helping our residents live longer, healthier lives and deliver the No. 1 quality care in the Nation. The medical loss ratio within the health reform law is holding all health plans to the same standards we have set in Minnesota by requiring that 80 to 85 percent of premium dollars actually pay for health services.

Before this year, in other plans throughout the Nation, less than 60 percent of the premiums were put toward health care. The rest was being used for administrative costs, for marketing, for bonuses, and for profits. In fact, one study of insurers in Texas a few years ago showed MLRs, medical loss ratios, as low as 22 percent—meaning that of all the premiums families were paying in to their insurers, the insurers were spending only 22 percent on actual health care services for them.

That is why my medical loss ratio provision is so important. It squeezes the fat out of the health insurance market and makes your premium dollars go farther. For many families it is actually lowering costs, delivering $1.1 billion a year in rebates. Those checks, $1.1 billion, are in addition to lowering the premiums. For example, the 10-percent reduction by Aetna in Connecticut. This was an incredibly important step because we know premiums were going up way too fast, a lot faster than those families' income. This is just one way the health care law is already changing the culture of care in our country.

One of the other things the law did was move toward rewarding quality of care, not quantity of care. It specifically directed Medicare to start paying doctors based on the value of the care they provide, not the volume. This is a provision that I and Senator KLOBUCHAR and several other of our colleagues championed, called the value index. That is because when Minnesota doctors get paid less for providing higher quality care, everyone else loses. Minnesota loses because Minnesota reimburses 50 percent less per Medicare patient on average in Minnesota than for each patient, on average, in Texas. So Minnesota actually gets punished for being No. 1. It gets punished for higher quality care with lower reimbursements. Patients in Texas lose because they are not getting the highest value care for their health care dollar. And all taxpayers lose when Medicare pays for unnecessary or overpriced service in Texas or other low-value States.

This is not about pitting Minnesota against Texas or other low-value States. It is about incentivizing the Texases to be more like Minnesota—which, again, has the highest health care quality in the Nation. That will begin to happen when the value index kicks in under this law.

It would be an understatement to say the law has received some attention this year, and I know there is a lot of uncertainty among our constituents about how the law will affect them. That is because sometimes there is a little misinformation put out there. I just had a colleague say there is nothing in the bill to address paperwork. That is certainly not true. In fact, I authored a provision on simplifying billing.

There is some misinformation on why IRS agents are there to look into your insurance—and anything done in the law to address workforce shortages. That is not true. There is an entire title on workforce. Sometimes people have to sort out what is being said on this floor. So there is some uncertainty.

Let me take a moment to talk about a few of the other things the law is already doing for the people of Minnesota. This is all in the law and happening. I am just telling what is going on right now.

First of all, starting tomorrow, August 1, 900,000 women in Minnesota and 47 million women around the country will have free access to preventive health services, including gestational diabetes screenings, preventive health visits with their doctors, and FDA-approved contraceptives. Because of the health care law, women, not their insurance companies, can now make decisions about their health care and can access the services that will keep them healthy.

The health care law is also helping families in Minnesota and across the country by prohibiting insurers from denying health coverage for children who have preexisting conditions. I have met children who are alive today because of this provision. As a parent, I know how grateful their parents are. Parents around the country can now sleep a little easier, knowing that if their child gets sick they will still be able to get the health care coverage they need. We should be celebrating that. This is not about putting the government between you and your doctor, as I hear sometimes. This is about getting an insurance company out of the way and making sure that children can get coverage.

And adults. We have seen the limitation of lifetime limits on care. Your insurance company can no longer put an arbitrary cap on your care. I have seen a gentleman whose life was saved because of this. Before this law came into being they could drop you—and they did. That is over. That is done. People do not have to worry about hitting an arbitrary limit and then being thrown off their insurance—because they have. We should be celebrating that. That is something that should be bringing a lot of relief to people. That is why we are going to be having far fewer bankruptcies.

Parents will also be relieved to know that young adults can now stay—they had been able to stay on their parents' health insurance plan until they are 26. Because of this provision, 35,000 young adults in Minnesota are now insured on their parents' policies.

I was at a senior center in Woodbury the other day. Seniors are very happy with the changes that the health care law has made. When I visit senior centers in Minnesota, I hear relief from seniors who now can pay for their medications thanks to the provision in the health care law which is closing the doughnut hole. The provision has already allowed 57,000 seniors in Minnesota to receive a 50-percent discount on their covered brandname prescription drugs when they hit the so-called doughnut hole, an average of $590 savings per person.

I can see the Presiding Officer nodding. I know she goes to senior centers in New Hampshire and knows when seniors hear that people want to repeal this they are miffed. I have actually been at a senior center when they said, What can we do? And they wanted to get up and go out and start being activists for the health care law when they heard that some of my friends want to repeal this.

Some of them are making it just on Social Security. Now the doughnut hole is closing and they like that. It means they can take their medication and it means they do not have to take it every other day or they don't have to cut it in half. My friends on the other side want to repeal it.

Seniors are also getting free preventive health services under the health care law, such as mammograms, colonoscopies, as well as free annual wellness visits to their doctor—and, boy, do they like that.

I could go on and on, but I will not. The point is, because of the law more people are getting care, the quality of care is better, and we are lowering costs. I am proud of that. As we here in the Senate head home to spend August in our States, I urge my colleagues to listen, as I do, when constituents tell

us about the rebates they received. I was on a plane two weekends ago. A woman showed me her check. The woman I was sitting next to showed me her rebate check.

I urge my colleagues to listen to constituents talk about the rebates they receive, the kids who are able to stay on their parents' insurance, the health screenings that save the lives of grandparents. I hope they will listen to the stories of kids with preexisting illnesses who were finally able to get coverage and seniors who were able to afford both their prescriptions and their dinner. I urge my colleagues to acknowledge these benefits and to support the continued implementation of the Affordable Care Act.

I yield the floor.

The PRESIDING OFFICER. The Senator from Delaware.

Mr. CARPER. Madam President, there are several people who wish to be recognized. If Senator COLLINS is ready to go, I will yield to her and then ask unanimous consent to speak immediately after her, then to be followed by Senator ALEXANDER, if that is the will of the body.

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

The Senator from Maine.

Ms. COLLINS. Madam President, first let me thank the Senator from Delaware for his graciousness. In light of the fact that there are so many people who are waiting to speak, I will be brief. But I want to talk about the legislation that is before us, the cyber security bill. This bill represents the Senate's best chance this year to pass urgently needed cyber security legislation.

Why do I say it is urgent? Virtually every national and homeland security expert, from President Bush's administration including President Obama's administration, has warned us repeatedly that a cyber attack is coming and it is an attack that is going to be aimed at our critical infrastructure. For us to let disagreements over exactly how to counter this threat prevent the passage of this bill would be a tragedy and could lead to a tragedy. This is serious.

Yesterday we had a meeting with the FBI, with the Department of Homeland Security, with GEN Keith Alexander, who is the head of cyber command, and the head of the National Security Agency. They were unanimous in warning us that Congress must act and must act now. Every single day nation states, terrorist groups, hacktivists, persistent hackers, transnational criminal gangs, are probing our cyber defenses. Intrusions are rampant. As one expert told me, there are really only two kinds of large companies in this country: those that know they have been hacked and those that do not know they have been hacked. It is so important that we act. I must say we are working very hard to try to accommodate the concerns that have been raised by some of our colleagues and by some in the business community. We, therefore, have altered our bill in a significant way.

Another charge I have heard thrown loosely around here is that somehow there has not been enough study; somehow there is not enough process; somehow we need more hearings. Our homeland security committee alone has had 10 hearings on cyber security—10 hearings. The Senate, as a whole, has had 25 hearings and numerous classified briefings. How many more briefings, hearings, and reports do we need? The head of the FBI, Robert Mueller, has told us that in his judgment the threat of a cyber attack will soon exceed the threat of a terrorist attack. Of course, they may be combined. It may be a terrorist group using cyber tools to launch an attack on this country. There is a Web site video that shows an arm of al-Qaida which encourages cyber attacks and talks about how easy it would be to conduct it.

Senator LIEBERMAN and I, along with our three principal cosponsors: Senator FEINSTEIN, Senator ROCKEFELLER, and Senator CARPER, have made significant changes in our bill to respond to concerns that have been raised. Most notably we have gone from having a mandatory framework to a voluntary approach to enhance the security of our most critical infrastructure. The underlying concept of this approach, which was suggested in a very constructive way by our colleagues Senator KYL and Senator WHITEHOUSE, is to encourage owners of our most critical infrastructure to enhance their cyber security by providing them with various incentives, the most important of which is liability protections. We have also made changes to improve the privacy protections and the information-sharing title of our bill.

The bill establishes a multiagency council, the National Cyber Security Council, to respond to concerns that too much power was being given to the Department of Homeland Security. So now we have an interagency body that includes the Department of Defense, the Department of Justice, represented by the FBI, the Department of Commerce, the intelligence community—undoubtedly it would be the Director of the National Intelligence Office—and appropriate sector-specific Federal agencies, such as FERC, if we are talking about how best to protect our electric grid.

The council would work in partnership with the private sector and would conduct risk assessments to identify our Nation's most critical cyber infrastructure. What do we mean by that? We hear that term. What exactly is critical cyber infrastructure? It is that which, if damaged, could result in mass casualties, mass evacuations, catastrophic economic damage to our country or severe harm to our national security. Don't we want to safeguard critical national assets that if damaged would cause numerous deaths, people to flee their homes, their communities, a disaster for our economy, or a severe blow to our national security? I can't believe there is even any discussion about the need for us to have robust systems to protect us against mass casualties, a devastating blow to our economy, and catastrophic consequences. That is a high bar in our bill for defining what is critical cyber infrastructure. It isn't every business in this country. Those who are implying that it is and that this is sweeping are not accurately reading the bill. We would be irresponsible if we did not act when the warnings are so loud and are coming from so many respected sources.

We have had the Aspen Institute Group on Cyber Security Issues endorse our bill and urge us to go toward its consideration. That is chaired by President Bush's Homeland Security Secretary Michael Chertoff and by a renowned expert on the other side of the aisle, former Congresswoman Jane Harman. It also includes people such as Paul Wolfowitz, not exactly a liberal activist the last time I checked, but certainly one who commands great respect for his knowledge in this area.

I am amazed we are letting the clock tick down when we know it is not a matter of if there is going to be a cyber attack on this country, it is a matter of when.

Let me very briefly address another issue. Is there some opposition among the business community to this bill? Yes, there is. But there is also a great deal of support from the business community. We have, for example, a letter from the NDIA, which represents 1,750 defense firms. We have letters of endorsement from Sysco, Oracle, the Silicon Valley Leadership Group, the Business Software Alliance, from Semantec, EMC Corporation, the Center for a New American Security, endorsements from individuals in the previous administration such as General Hayden, Mike McConnell, and Asa Hutchinson. There are many supporters for this bill. It is not surprising because they know how important it is that we act.

Ms. COLLINS. In closing, I wish to read a little from General Alexander's letter, which is dated today. In it he says:

> I am writing to express my strong support for passage of a comprehensive bipartisan cyber security bill by the Senate this week. The cyber threat facing the Nation is real and demands immediate action—

Not action next year, not action next Congress, not action even after the recess we are about to take. As General Alexander says:

> The time to act is now; we simply cannot afford further delay. Moreover, to be most effective in protecting against this threat to our national security, cyber security legislation should address both information sharing and core critical infrastructure hardening.

That is exactly what the bill we have brought before the Senate would do. I urge our colleagues to join us. If they have other ideas, offer amendments, but let's get on with the task before us

before we are looking back and saying: Why didn't we act? Why didn't we pay attention to all of those warnings?

The PRESIDING OFFICER. The Senator from Delaware.

Mr. CARPER. Madam President, while the Senator is still on the floor, I wish to engage in a brief colloquy, adlibbing this or, as I recall in football, an audible. We have the two people who are most key to this, Senator LIEBERMAN, chairman of our committee, and Senator COLLINS, our ranking member, who worked very hard with their staff and our staffs to fashion this legislation.

In recent years when we heard opposition to doing something on cyber security, the concern we had was there was going to be a top-down. There was going to be Homeland Security, which in its early days did not have a very good reputation. The idea was that somehow Homeland Security was going to be running this top down without a whole lot of input from industry. Basically we have taken even the second most recent version of our bill, and we changed that. What we said is it is not going to be top-down, it is not going to be Homeland Security saying these are the best practices, these are the standards to protect cyber security. Instead we said: Industry, what do you want to tell us? ''Us'' being Homeland Security, ''us'' being the Department of Defense, ''us'' being the National Security Agency, ''us'' being the FBI. What do you think those best practice standards should be? Give us a chance to work on those together.

Correct me if I am wrong, but I don't think the deal here is for Homeland Security to say: You have to throw those away; those make no sense, we will do it our way. That is not what is going to happen here.

In our meeting yesterday with the folks from the FBI and the National Security Agency, that is not the way it is going to work. It is not the way it works today and it is not the way it is going to work in the future. What does the Senator think?

The PRESIDING OFFICER. The Senator from Maine.

Ms. COLLINS. Madam President, if I could respond through the Chair to my colleague from Delaware, he is absolutely correct, this is a collaborative partnership with the private sector, and indeed, it has to be. Eighty-five percent of the critical infrastructure is owned by the private sector, so it makes sense to have their involvement. We restructured the bill to require that, and there is another safeguard. Since this is a voluntary system we have now devised, adopting the Kyl-Whitehouse approach, if the private sector decided not to participate, it essentially invalidates the standards that are developed. So why would this interagency council, which has developed the standards based on the recommendations of the private sector, not adopt reasonable standards? They want industry to participate. That is the ultimate safeguard, I say to my colleague from Delaware and my colleague, the chairman from Connecticut, who also may want to add to this.

The PRESIDING OFFICER. The Senator from Delaware.

Mr. CARPER. I am going to direct this question to our chairman through the Chair. One of the other criticisms of the early version of the bill was not only was it top-down oriented and directed by Homeland Security, but also there were just sticks involved. We were not going to incentivize anybody to comply with the standards that might be developed, but we would just hammer somebody. That is not the way it turned out. I commend the chairman for doing that.

Will the chairman lay out for us in a minute or two how it would work? I think it is a much smarter approach.

The PRESIDING OFFICER. The Senator from Connecticut.

Mr. LIEBERMAN. I thank my friend from Delaware for the question. This is now a voluntary system and there is a lot to be said about that.

I want to go back to that meeting yesterday. We had a broad bipartisan group of Senators who have been most active, but from different perspectives, on this question of cyber security legislation who met yesterday with the key cyber security officials in our government from the Department of Defense, Department of Homeland Security, FBI, and the National Security Agency. I am going to explain why we went to the carrots and took out the sticks by saying, in general terms, these experts—not political people, these are pros who deal with cyber defense—were asked by one of the Senators: What will happen if we don't adopt this legislation or something like it this session?

The cyber security professionals said to us: Our Nation will be more vulnerable to cyber attack.

In other words, this legislation contains authority to share information between the government and the private sector, between two private sector companies, that can't be done now. That is critically necessary to improve our defenses. The requirement of standards being promulgated as a result of a—or resulting from a public-private collaborative operation and then offering the carrot of immunity from liability is something that doesn't exist now. All the experts say, though some of the private sector operators of critical cyber security infrastructure—we are talking, again, about the companies that run the electric grid or the telecommunications system or the entire financial system or dams that hold back water; we are not talking about ma-and-pa businesses back home—some of them are doing a pretty good job at defending that cyber infrastructure, but most of them are not doing enough. That is where the government has to come in and push them in that direction.

Why did we change it from mandatory to voluntary, from sticks to carrots? Because we didn't have the votes to adopt the mandatory, which I think is necessary. Because of the urgency of the threat, as I just reflected that we heard yesterday from the professionals in this area, we said—Senator COLLINS and I, Senator ROCKEFELLER, Senator FEINSTEIN, Senator CARPER—OK, we are not going to get 100 percent of what we want around here, and we understand that, so let's settle for 80 percent. Perhaps the other side will feel they got 80 percent. But what is most important is that we will get something done to protect our security.

I must tell my colleagues we are at a point now in this debate, with the kind of never-ending questions about every detail, not withstanding all the compromises Senator COLLINS, Senator CARPER and I have made and the filing of an amendment by Senator MCCONNELL to repeal ObamaCare—we can have a position on ObamaCare, but to put it on this cyber security bill is not fair, not relevant, not constructive.

I think we are coming to a moment where we are going to have to face a tough decision. I have talked to the majority leader about filing for cloture soon so we can draw this to a choice: Do our colleagues want to act to protect our cyber systems in this session or do they not? That is a tough choice, particularly if a Senator votes no, to have to explain, in light of all the evidence of the constant cyber attacks going on now and the cyber thefts of hundreds of billions of dollars from our industries and tens of thousands of jobs lost as a result to foreign countries, if the Senate is going to say, no, we don't want to take that up now. I hope and pray that is not the case.

The way this is moving right now, this last week of the session before we break, I am afraid we are headed in the wrong direction, and we don't see the kind of willingness to compromise that ought to be there. We are tested again in this Chamber: Are we going to fix national problems? It is hard to do on some of the fiscal issues we have turned away from, but on this one, traditionally, when it came to our national security, we have put the special interests aside and together dealt with the national security interests. I fear at this moment, in response to my friend from Delaware, that is not the direction in which we are going. I hope I am wrong. I am, by nature, an optimist, but right now I am a pessimist.

I yield the floor.

The PRESIDING OFFICER. The Senator from Delaware.

Mr. CARPER. My colleagues have heard me say this before. We have been joined by Senator ROCKEFELLER, who has done great work, Senator FEINSTEIN, and others, Democratic and Republican, who have done fine work on this legislation.

But I love asking people who have been married a long time: What is the secret to being married a long time?

This is especially important for me to say this with Senator COLLINS sitting on the floor. She and certainly her husband to be anticipate their coming marriage. But I love asking people who have been married a long time: What is the secret to be being married a long time? I get great answers, funny answers but also some very profound ones, and the best thing I ever got was the two Cs. What are the two Cs? Communicate and compromise. That is not just the secret for a long marriage, a union between husband and wife, but it is also the secret for a vibrant democracy.

I think the two Cs characterize what is going on with this legislation because I have been here a while—11 years—and I don't know that I have ever seen better communication on an issue of this importance than I have in this instance. It was very dramatic, very satisfying, and frankly, compromise, the kind of compromise we have talked about over the last 15 minutes or so, needed, given, done willingly, to lead us to this point today.

It has been said before, and I will say it again. The reason we are on this bill today, why we have taken it up today, this week, is because our economy and our national security are under attack. This is not the kind of war that some of us served in during our youth. This is not the kind of war we have read about in history books. It is not the kind of war we have seen and watched on TV. This war is occurring in cyber space, and it is occurring in real time.

Literally, as I speak, it is being carried out by sophisticated criminals, by terrorists, and even by other countries. While some hackers just want to cause mischief or make a political point, others want to hurt people, our people. Still others want to steal our ideas, our intellectual property, as well as other sensitive information. From clean energy technologies and defense systems to medical research and corporate mergers, cyber spies are looking to steal some of the very innovations that fuel our economy and help make us a great nation.

GEN Keith Alexander, the commander of U.S. Cyber Command, has called these efforts the greatest transfer of wealth in history. Those of us who have tried to put a dollar figure on how much intellectual property we are losing to cyber theft have put the pricetag at about $¼ trillion per year. It is not just valuable information we are losing. To put it bluntly, it is American jobs, and it is our competitive edge.

Of course, the same vulnerabilities being exploited to steal our intellectual property can be used by those who want to attack us to do physical harm. With a few clicks of a mouse, cyber terrorists or a sovereign nation could shut down our electric grid, they could shut down manufacturing, they can release dangerous chemicals into our air, they can release dangerous chemicals into our water supply. They could disrupt our financial systems. At the very least, any one of these attacks could further slow the economic recovery of our country or disrupt it altogether.

In a worst-case scenario, a particularly lethal cyber attack could throw parts of our country into chaos or even lead to widespread loss of life. If my colleagues don't believe that, look at the impact the recent summer storms and the resulting power outages had on this region. If we don't become more vigilant and soon, a sophisticated hacker can succeed in replicating that kind of power outage, putting many lives in danger and severely undercutting the productivity of our workforce.

The revised bill we take up today takes a number of bold steps to better secure our critical infrastructure and share cyber threat information. It will go a long way toward bringing our cyber capabilities into the 21st century. It represents a good-faith effort to address legitimate concerns of business and privacy groups of our intelligence community and of Senators on both sides of the aisle.

None of this bill's five original cosponsors is suggesting our bill is perfect. As my colleagues hear me say from time to time, if it isn't perfect, make it better. With that thought in mind, we look forward to working together with all our colleagues to find common ground to make this legislation even better.

For example, many of my colleagues and I are concerned that we don't have the proper safeguards in place when private information, ranging from Social Security numbers to financial records, are compromised. The American public expects that government agencies and private businesses holding our tax information, our medical records, and other sensitive data will take every precaution necessary to ensure that sensitive information is secure and well protected. Too often those expectations are not met.

That is why I have introduced a bipartisan amendment with my colleague Senator BLUNT to address concerns regarding data breaches which occur all too often. Our amendment would ensure that Americans can be confident that their private and sensitive information is made more secure. As our Nation becomes increasingly reliant on technological advances to do just about everything, it is imperative that we not let technology outpace our ability to prevent fraud and identity theft.

However, with the recent breach within the Federal employees retirement program—the Thrift Savings Plan—over 100,000 Federal participants know all too well that their sensitive private information is not always safeguarded as it should be.

The amendment Senator BLUNT and I are offering seeks to ensure that all entities holding personal sensitive information have to adhere to a national standard that is designed to keep that information safe while ensuring that both consumers and law enforcement are promptly notified in the event of a breach. This requirement would replace the current patchwork of 46 separate State laws while ensuring that consumers have a uniform set of protections they can understand. By adopting this data-breach amendment and passing the broader cyber security bill, we will enable the United States to lead by example both in preventing cyber attacks from occurring in the first place and in responding swiftly and effectively to protect consumers in the unfortunate event of an attack or a breach.

As we consider our amendment, the Blunt-Carper amendment, let's remember that this bill is not the finish line. If I can paraphrase Winston Churchill, this is not the end. This is not the beginning of the end. This bill really represents the end of the beginning. And as beginnings go, it ain't bad.

Although we are still working out a compromise, I want to close by talking very briefly about some of the features of the underlying bill we are considering.

First—I will reiterate what has been said before; it bears repeating—we have elected not to direct the Department of Homeland Security to mandate new cyber security regulations for private owners of critical infrastructure. We said we are not going to do that. Instead, we have endorsed an approach that relies on a public-private partnership and a voluntary cyber security program to strengthen the electronic backbone of our most sensitive systems. Instead of government penalties, our bill calls for using incentives such as liability protection to encourage critical infrastructure owners to adopt voluntary cyber practices developed by industry.

Second, our revised bill provides a framework for the sharing of cyber threat information between the Federal Government and the private sector while offering liability protection and better privacy protections for all Americans.

Third, to ensure that Federal agencies are better equipped to stop cyber attacks on them, the bill includes a number of security measures that I have worked on for years with Senator COLLINS and others to better protect our Federal information systems. In particular, this bill will help replace our outdated, paper-based security practices with a real-time security system that can actively monitor, detect, and respond to threats. For example, agencies will be required to continuously monitor their systems the way a security guard would watch a building through a video camera rather than just taking a snapshop, developing the film, and reporting on the results once a year.

Finally, our bill makes a number of important investments in developing the next generation of cyber security professionals. This is workforce development. For example, the bill provides stronger cyber security training and

establishes better cyber security programs in our schools and in our universities. This legislation also makes research and development for cyber security a priority so we can develop cutting-edge technologies here at home and bring jobs to our country. Doing so will not only make us safer as a nation, it will help ensure that America's workforce is better prepared for tomorrow's job market, and tomorrow is just around the corner.

I wish to conclude my remarks here today with something that one of our colleagues, MIKE ENZI of Wyoming, introduced to me several years ago. MIKE calls it the 80–20 rule. He used it at the time to explain to me how he, one of the most conservative Republicans in the Senate, and the late Ted Kennedy, one of the most liberal Democrats in the Senate, were able to accomplish so much prior to Ted's death when they were the two senior leaders on the Senate Health, Education, Labor, and Pensions Committee.

I said to Senator ENZI: How come the two of you, very different people—one a Democrat and one a Republican—were able to get so much done?

Senator ENZI said to me: Ted and I agreed on about 80 percent of what needed to be done on most issues, and we disagreed on the other 20 percent. Somewhere along the way, we just decided to focus on the 80 percent we agreed on and set the other 20 percent aside for another day.

The cyber security legislation we are debating here today this week is an 80–20 bill. I think it is worth asking, is it worthwhile to pass a bill that achieves maybe only 80 percent of what we want to do or even only 70 percent of what we want to do? I would just say, well, compared to what? Compared to doing nothing? Compared to zero? Given all that is at stake in today's dangerous world, you bet it is worthwhile. That much we ought to be able to agree on, so let's get it done.

Like many of my colleagues who have worked on the legislation for years, I welcome the opportunity this week to legislate—to legislate—on an issue of great importance to our Nation, to offer our amendments, to debate them, to defend them, to vote on them, make this bill better by doing so, and in the end adopt this bill as amended by a bipartisan margin. A lot of people in this country of ours question today whether we are still able to set aside our partisan and other differences when the stakes are high and summon the political will to do what is best for America. Let's show them by our actions this week that, yes, we can. Let's seize the day. Carpe diem.

With that, I yield the floor.

The PRESIDING OFFICER. The Senator from Connecticut.

Mr. LIEBERMAN. Madam President, I ask unanimous consent that the period for debate only on S. 3414, the Cybersecurity Act, be extended until 6:30 p.m.; further, that the majority leader be recognized at 6:30 p.m.

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

The PRESIDING OFFICER (Mr. WHITEHOUSE). The Senator from New York.

Mr. SCHUMER. Mr. President, first, I wish to salute my colleague from Delaware. We have a number of people in this body who will take on the very tough issues—issues, frankly, that can only succeed when there is bipartisan agreement but that are deep and complicated and take day after day, week after week, even month after month of effort—and there are not many who can craft that type of legislation. The Senator from Delaware is one of them. He did it on the postal bill. He is doing it here on cyber security. I believe on both of them he will have ultimate success, and we thank the Senator. We thank him for his good work.

Now I would like to discuss the cyber security bill. I am very hopeful that we will pass a bill that will find a good and workable balance—one certainly that ensures that our critical infrastructure has the most effective countermeasures to prevent cyber attacks but one that will also encourage our dynamic technology industry to continue to innovate, and protect freedom of expression and privacy on the Internet.

Let me remind my colleagues that the Internet was originally developed as a way for universities, governments, and companies to collaborate on research and other projects. The whole purpose of the Internet was meant to stimulate the open exchange of ideas, and as a result it has changed the world. We have seen it in Egypt, in Russia, in China. We have seen the Internet—people's ability to communicate, unfettered by government or other strong forces—create huge amounts of power—good power, positive power.

Just ask the entrepreneurs who developed whole new ways of selling products and developing services about how the Internet was made to stimulate the open exchange of ideas. It has given the opportunity to someone with an idea to actually take that idea and turn it into a business because it so reduces the transaction costs of doing so. Just ask the inventors and creators who have fostered new means of expression, allowing us to communicate in real time, efficiently and inexpensively, with our colleagues all over the world.

I am an efficiency bug. I like to use ''I am a busy fella.'' I love the work I do, and I like to use it as efficiently as possible—the fact that I can have a laptop or an iPad in the car while the car is driving forward. I am not driving; I am sitting there working. In the old days, you could not do that. It is amazing how it has improved our efficiency. It is sort of, in a certain sense, Adam Smith's dream because it reduces transaction costs and allows us to focus effectively on producing what people want and need.

In short, our cyber world is one we could have never imagined 30 years ago. It is both simple—it can be accessed through a few keystrokes or screen touches—and yet it is enormously complex in its infrastructure. We have to do everything we can to protect that free and open access—that is the theme of my speech today—although we also, of course, have to protect the critical infrastructure behind it.

We are all aware of the national security risks if we do not do a cyber bill. Many of us have sat up in the Visitor Center, in the secure room, and heard leaders of our military and intelligence agencies tell us that the greatest threat to America is a cyber attack on our critical infrastructure—in many of their estimation, even more dangerous than terrorism.

Hackers broke into the Pentagon's F–35 Joint Strike Fighter project, stealing the aircraft's design and electronic-related schematics. It is not hard to imagine a scenario where hackers break into a gas refinery or a nuclear powerplant to wreak havoc with the control computer systems, nor is it hard to see a scenario where Iran attempts to learn some of our nuclear secrets. So it is very important to deal with the critical infrastructure piece.

Mr. President, let me commend you for your hard work in this area, along with the Senator from Arizona. We are still hoping and praying you guys can come to an agreement, along with the help of many. I know Senator MIKULSKI has been very active and many other of my colleagues, but the Presiding Officer's leadership has been exemplary as well, and I would apply the same words to you that I applied to the Senator from Delaware before in terms of working on complex, difficult projects and moving forward with them.

Anyway, it is so very important that we protect our infrastructure, but at the same time—and this is what makes the legislation even more difficult—we have to be aware of the risk to a critical part of our economy if we do not do it right, if we do not do it carefully, if we do not do it thoughtfully, and if we do not balance the need to protect infrastructure with legitimate rights of the freedom of the Internet and of privacy.

To be perfectly frank, I have a big dog in this fight. You see, the Silicon Valley may have given us the semiconductor, but New York City, in my opinion, will be the birthplace of the next great generation of Internet giants. New York entrepreneurs started Foursquare, Tumblr, and Kickstarter. CodeAcademy, TechStars, and General Assembly are training the next generation of Internet entrepreneurs. Venture capital is flocking to New York to help these startups. For the first time, we are getting engineers and scientists who want to be in New York. We are still not at the level of the Silicon Valley, but we are probably No. 2 in the country in this regard, and, like all New Yorkers, we want to be No. 1 at some point.

What is more, the existing Internet giants—Facebook and Google and Twitter—have all opened major offices in New York City. Google has over 3,000 people. I was proud to be at the opening of Facebook, and they are so happy with their office, they are expanding its role already. These companies know the talent and energy that are unique to New York, and they do not want to miss out on the next great idea. That, as I said, is likely to come from New York.

These ideas are not just important for New York but for America. Internet and tech companies around the country have ushered in a new era of change. They have made our world a drastically and dramatically different place than it was even 10 years ago—a better world, a more open world, a more productive world.

But one thing remains the same: We do not have a coherent and comprehensive national strategy to protect the critical networks that power our everyday lives—our homes, our businesses, and our computers. It is akin to protecting the Taj Mahal with a chain link fence and a bike lock. These networks protect our water systems and our financial information, the electric grid and our e-mail accounts.

This bill goes a long way in establishing a set of principles and programs that will make these vulnerable networks safer, but there are some parts of the bill I fear go a step too far in the name of security over privacy, and there has to be a balance. The same minds who have given us the great Internet innovations of the 21st century have told me, convinced me, educated me that we cannot cede too much power to one side of this equation.

We all know that in this very complex cyber world, we do give up some of our privacy, but unabated authority to stifle innovation in the name of cyber security is a bridge too far. That is why I am happy to cosponsor the amendment of my colleague from Minnesota AL FRANKEN. He has become an expert on trying to figure out how we can preserve the dynamism, the effectiveness, the efficiency of the Internet but at the same time preserve our privacy.

As more and more of our economic lifeblood has shifted into the cyber world, we have an obligation to ensure that the infrastructure that validates credit card purchases, directs planes, and controls electricity is well protected against cyber attack. It is not a secret that people want to disrupt our way of life, and it is easy to imagine a world where terrorists attempt to take control of railroad switches and traffic lights to cause incredible disruption to our everyday lives. However, we must make sure that in protecting what we have, we do not stifle innovation, we do not trample on people's privacy rights. We have to leave room for the creation from the next Steve Jobs, Bill Gates, or whomever, while protecting the security the average middle-class family, the Baileys, feel when they go online to buy birthday presents for their grandchildren.

So in the final bill, we must find the right balance to preserve the economic viability of the Internet; otherwise, there will be no critical infrastructure to protect. But we must protect privacy rights, and I think the Franken amendment—and I commend it to my colleagues; a lot of work has gone into it—puts the balance in the right place.

I hope that as we move forward on this bill—either now or in September when we return—we will get broad bipartisan support for that amendment because it enables us to, in a certain sense, have our cake and eat it too: protect our infrastructure but at the same time protect, nurture our creativity and the openness of the Internet and protect our privacy.

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

The PRESIDING OFFICER. The Senator from Nebraska.

THE FARM BILL

Mr. NELSON of Nebraska. Mr. President, the worst drought in 50 years has hit Nebraska and the entire Midwest hard. Every single one of Nebraska's 93 counties is in a state of severe drought.

If you look at the chart I have in the Chamber, you can see that the drought is throughout the Midwest, into the Middle East, down into the Southeast, down into Texas and the West, even drought conditions in Hawaii, and it is abnormally dry up in the northern part of Alaska. The USDA has already declared more than 40 Nebraska counties as natural disaster areas. If you take a look at this picture, you can see the cornfields that are just completely dirt fields now; pasture that is nothing more than dried grass, where there is still grass and dirt; the soybean fields are decimated; and corn is in many areas not only dwarfed in its growth but is not producing ears of corn. The bone-dry conditions continue to damage corn, soybeans, pastures, and rangeland, even as we speak.

Just last week a small blaze quickly spread over the parched land in north central Nebraska. It rapidly grew into a fire that consumed tens of thousands of acres, 14 houses, and forced many others from their homes.

Nebraska is fortunate to have had hard-working firefighters in our State and others to put out those flames. Hopefully, we will not need to utilize their talents in the near future. Now what Nebraska needs is disaster relief. And we are not alone. If you look at this chart, you will see that a good part of the rest of the country needs disaster relief as well. Unfortunately, the disaster programs in the 2008 farm bill have already expired.

While the Senate passed the 5-year farm bill in June, the House is not even expected to take action on it. The Senate's 5-year farm bill strengthens and improves the 2008 farm bill, particularly the natural disaster relief provisions. It beefs up and rehabilitates livestock disaster programs, it provides tools to help reduce fire risk and improve forest health, it improves and increases access to crop insurance to protect against future natural disasters, it authorizes direct and guaranteed loans for recovery from wildfires and drought, and the list goes on—all important programs necessary to deal with this disaster we are facing in our country today.

The Senate's 5-year farm bill makes necessary upgrades to the policies in the 2008 farm bill to help Americans recover from natural disasters, and it does it without digging the country deeper into debt. The Senate passed this bipartisan farm bill in June, but the House will not take action on it. Plus, the House is expected to move a separate bill, essentially a 1-year extension of the old 2008 farm bill. A 1-year extension of outdated and inefficient policies is not adequate, it is irresponsible. We need the substantial reforms in the Senate's 5-year farm bill now. A 1-year extension of current policy does nothing to help those who need the farm bill and its disaster relief the most. When you can do better, you should do better.

Congress passed a 5-year farm bill in 2008, 2002, 1996, 1990, 1985—you get the picture—just about every 5 years between 1965 and today. Surely the House can pass a proper 5-year farm bill. And the need to is all the more apparent in the face of the nationwide drought, with the disaster relief provisions in the 2008 farm bill having expired on September 30 last year, 2011.

Now, instead of passing a 5-year extension of the farm bill, they have held a lot of political messaging votes and they put off doing what should have been done at the very beginning. And now, while America is getting hit by drought and fire, while American farmers and ranchers do not have the disaster relief because there is no farm bill, the House is merely going to pass a 1-year extension of current policies. They want to buy some time, kick the can down the road.

Well, now it is time for the House to do its job. Do what is right for the country. Do not take the easy way out. Show the American people that you remember why you are here and what you need to do and can actually do it. Americans do not want a flimsy 1-year extension of inadequate coverage and outdated policies. Americans want a dependable, modern, and economical 5-year farm bill that cuts Federal spending. That is what the Senate gave the House. That is what the House Agriculture Committee gave the House to work with—its own 5-year plan. Sure, there are real differences between the Senate bill and the House Agriculture bill, but there should be room for consensus. So the House must pass the bill or pass our bill, but do not pass a 1-year extension of outdated policies that will not work for modern American agriculture. Do not try to just coast along without a 5-year farm bill.

The lack of a 2012 farm bill will fail to provide certainty to farmers and ranchers and lead to higher prices for all consumers at the grocery store. And this is on top of the already predicted 3 to 4 percent rise in food prices caused by the drought. We do not want that and America deserves better. Nebraska's farmers and our American farmers and ranchers and all those affected by the drought are depending on Congress to do our job right and fairly debate this issue. So do not kick the can down the road.

I urge the House to bring a 5-year farm bill to the House floor as soon as possible.

I yield the floor.

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

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

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

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

Mr. LIEBERMAN. Mr. President, I rise to continue the discussion on the cyber security legislation, and particularly S. 3414, the pending business before the Senate, which is the Cybersecurity Act of 2012, the bipartisan piece of legislation to deal with an urgent national crisis.

I want first, again, to speak to our colleagues about the seriousness of the threat. I think sometimes that because most people haven't experienced the consequences of a cyber attack—and most are not aware of the constant cyber theft going on with moving money from bank accounts and stealing industrial secrets—frankly, a lot of the businesses that are victims of the theft don't want to acknowledge them or announce them for fear of exposing their own lack of adequate cyber defenses, but also a kind of general embarrassment. Yet we now know as a public matter—whether it has sunk into the consciousness among most of the American people—that some great companies that are very tech savvy, cyber savvy, have been the victims of cyber attacks.

Sony, RSA, Google, and others have come momentarily to public attention, but I think what this has meant has been unclear to people. It may, in fact, be unclear to many of the leaders of the private corporations that control so much of our critical cyber infrastructure.

In America, 80 to 85 percent of the critical infrastructure is privately owned. That is the American way. That is the way it ought to be. But it means when the private sector owns critical infrastructure which can, and will be, a target of hostile action, enemy attack in this new world of ours, then we have to create a partnership with the private owners of this critical infrastructure to raise our defenses because it is not just their businesses they are defending, it is the security of the United States.

A chief information officer at one of the businesses that owns part of our critical infrastructure said to me at one point that it is hard to get the attention of the CEO on this problem. The CEO is balancing a lot of considerations, looking at annual budgets and quarterly profits. For the average CEO, the threat of cyber attack is distant. For the average chief information officer, it is not so distant.

As the majority leader pointed out earlier, I think it may help to look at something very difficult to look at, which is what is happening in India today where the power system has collapsed for hundreds of millions of people. That is a breakdown, as far as we know—and I believe that is what is the fact—that is a breakdown in parts of the electric grid.

Let me give another example. Last year, in Connecticut, we had a very serious early winter storm where there were still a lot of leaves on the trees; the branches were heavy. A lot of trees fell and took out a lot of power lines in our State. A lot of people were without power for days and days and days. Public buildings were used as shelters for the homeless. Elderly people, particularly, were affected with food spoiling in the refrigerators, the lack of lights in their dwelling, et cetera.

Just imagine for a moment if that was not the result of a weather event but of a cyber attack. Cyber systems are controlling the electric power grid, and I believe they are vulnerable. I think the same of a lot of the other cyber systems that control critical infrastructure in our financial system. The computer systems we depend on for the movement of money from one account to the other, the direct deposits we do, the money in our accounts, the billions of dollars that move between financial institutions every day—what would happen to our country if those systems were knocked out or what would happen if Wall Street and the stock exchanges were knocked out?

Again, as I said earlier today, think about the real nightmare situation, which is that a dam controlled by a cyber system is penetrated by an enemy who opens the dam and unleashes water, and torrents of water knock out communities in the path of that water and kill a lot of people. That is all, unfortunately, the age that we live in and the vulnerability we have.

There was a story in the Washington Post—I believe I talked about it before in this debate, but I will repeat it—about a young man on the other side of the world sitting at his computer at home. He was nothing special, but he was smart and computer savvy. He broke into the computer-controlled system—the cyber system controlling a small water utility in Texas. He had the ability to disrupt the functioning of that entire utility. He didn't do it, thank God. He posted online what he had done—a warning at least, perhaps a bit of bragging that he was able to do it. But think about an enemy who had hostile intent against the United States who would launch similar attacks against several small utilities around the country—or large utilities, for that matter.

Mr. President, last week, the people who are the real experts on cyber space gathered in Las Vegas at the annual—and this is an interesting title—Black Hat Computer Security Conference. They issued yet more warnings.

The conference opened with a very strong warning from Shawn Henry who, until recently, was the Assistant Director of the FBI in charge of the FBI's considerable cyber program. Some people call Shawn Henry the Nation's top cyber cop. He said this at the Black Hat Conference:

> The adversary knows that if you want to harm civilized society—take their water away, do away with their electricity. There are terrorist groups that are online now calling for the use of cyber as a weapon.

He went on:

> People will not truly get this until they see the real implications of a cyber attack. For example, people knew about Osama bin Laden prior to 9/11, but that awareness had risen by several orders of magnitude after the attacks.

Mr. Henry, former director of cyber programs at the FBI, concluded:

> I believe something like that will have to happen in the cyber world before people truly get it.

Obviously, we all hope and pray not, but at this moment in this debate, in the Senate's consideration of the Cybersecurity Act, there are a lot of inflexible positions that are being taken. People are not willing to come together across ideological and political divides to deal with a problem and a threat that faces us all. I fear that Mr. Henry may well have been right.

Mr. President, I urge my colleagues, don't run the risk that it will take a cyber 9/11 to bring us rushing back here to adopt cyber security legislation. It doesn't take much to imagine what will happen if we are the victims of a major cyber attack. Minor cyber attacks are happening every day. Major cyber thefts occur regularly in America every day. Let's heed the warning and come together over special interests to meet a national security interest and challenge.

I yield the floor and suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The assistant legislative clerk proceeded to call the roll.

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

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

Mr. NELSON of Florida. Mr. President, there is such an important subject that is looming over the country right now that Congress can do something about; that is, the possibility of

cyber attack. We have had this discussed by a number of people in very high and responsible positions and the threat is real.

What the threat means to all of us in our everyday lives is that electrical systems could be shut down, water systems could be shut down, the banking system could be shut down, sewer systems could go awry, and we can go on and on. For months we have been stymied from passing anything because of a disagreement in the business community, which is going to be one of the main recipients of a potential cyber attack.

I will choose my words very carefully as a member of the Senate Intelligence Committee and say this potential attack is real. It is real not only from rogue players but also some state actors, and we need to get this legislation up and going. I am most encouraged to think we are at a position to get agreement; that the chairman and vice chairman of our Intelligence Committee are going to come together in an agreement. We need to pass this—this week—because this is deadly serious.

I refer to a letter that has been made public from the commander of Cyber Command, a four-star general, GEN Keith Alexander. He is also the head of the National Security Agency. He has done a remarkable job. He sent a letter, dated today, to the majority leader imploring the Senate to move.

Whatever disagreements there have been over the concern of the Department of Homeland Security being the interfacing agency can be worked out. The National Security Agency—which almost all of us have enormous confidence in—is going to be directly involved.

It is my hope and I am expressing optimism that we are going to get this legislation out of here and to the House. If they can't pass it before this August recess, at least we can have some items over the August recess start to be informally conferenced to iron out any differences between the House and the Senate.

The PRESIDING OFFICER (Mr. BENNET). The Senator from Rhode Island.

Mr. WHITEHOUSE. Mr. President, I am here this afternoon to speak about the Cybersecurity Act of 2012, the measure that is on the Senate floor right now. This important bill addresses a serious and immediate threat to our Nation's security. I served 4 years on the Intelligence Committee during which I worked hard to understand the cyber security threat. I helped Senator MIKULSKI and Senator SNOWE write the Senate Intelligence Committee Cyber Security Report. I am the chairman of the Judiciary Subcommittee on Crime and Terrorism that has jurisdiction over cyber security. As I have explained before on the floor of the Senate, the cyber threat against our Nation—against our intellectual property, against our privacy, and against our safety—is vast and it is upon us. It is a national security threat. It is a national economic threat. We cannot afford to wait to pass legislation to respond to this threat. The leading national security experts in each party agree: Now is the time to pass comprehensive cyber security legislation.

The Cybersecurity Act of 2012 is a strong, comprehensive bill that will make our Nation safer. It will provide for the sharing of threat information between the government and private sector, and it will provide for the hardening, for the protection of the networks of the private companies that operate America's critical infrastructure—that run our electric grid, that run our financial networks, that run our communications systems and the other infrastructure that is essential to conducting the day-to-day way of life Americans enjoy, that is essential to our national security and to our economic well-being.

The Senate voted to proceed to this bill in a very broad, bipartisan manner—84 votes, as I recall. It has been disappointing in the wake of that that some elements within the business community are failing to cooperate, are failing to, for instance, provide constructive suggestions in areas where they have disagreement with this important legislation. Indeed, some appear intent on just preventing the Senate from passing legislation that would make us all safer.

In some cases these interests are not negotiating to get a bill that protects their interests. They are blockading to stop a bill that will protect all of our interests. To put this blockade into context, consider the views of GEN Keith Alexander, the Director of the National Security Agency and of United States Cyber Command. General Alexander is the most senior and respected cyber security expert in our Nation's military. He runs our two most technically sophisticated and skilled cyber operations. Today he wrote:

> The cyber threat facing the Nation is real and demands immediate action. The time to act is now; we simply cannot afford further delay. Moreover, to be most effective in protecting against this threat to our national security, cyber security legislation should address both information sharing and core critical infrastructure hardening.

The Cybersecurity Act addresses both of those issues, information sharing and core critical infrastructure hardening. It does what our military's leading cyber security expert says is necessary to be done to protect the Nation.

That, then, is the view of the leader of our military cyber warriors and cyber defenders based on both deep experience and access to the most deeply classified information held by the U.S. Government.

In contrast, industry arguments against cyber security legislation appear to have been developed with little or no awareness of the threat facing our Nation. Kevin Mandia of the leading security firm Mandiant has explained, for example, that ''in over 90 percent of the cases we have responded to, government notification was required to alert the company that a security breach was underway. In our last 50 incidents, '' he said, ''48 of the victim companies learned they were breached from the Federal Bureau of Investigation, the Department of Defense, or some other third party.''

The FBI's experience was similar. When the FBI-led National Cyber Investigative Joint Task Force informs the corporation it has been hacked, 9 times out of 10, the FBI reports, the corporation had no idea.

In Operation Aurora, the cyber attack which targeted numerous companies, only 3 out of the approximately 300 companies attacked were aware that they had been attacked before they were contacted by the government.

These are not unique incidents. Globally, I have said, General Alexander has said, and others have said that America is right now on the losing end of the largest illicit transfer of wealth in human history through cyber attack and through the theft through cyber attack of our intellectual property. So this is an industrywide problem.

Even the U.S. Chamber of Commerce has been the completely unwitting victim of a long-term and extensive cyber intrusion. Just last year the Wall Street Journal reported that a group of hackers in China breached the computer defenses of the U.S. Chamber, gained access to everything stored on its systems, including information about its 3 million members, and remained on the U.S. Chamber of Commerce's network for at least 6 months and possibly more than a year. The chamber only learned of the break-in when the FBI told the group that servers in China were stealing its information.

Even after the chamber was notified and increased its cyber security, the article stated that the chamber continued to experience suspicious activity, including a ''thermostat at a townhouse the Chamber owns on Capitol Hill . . . communicating with an Internet address in China . . . and . . . a printer used by Chamber executives spontaneously . . . printing pages with Chinese characters.'' These are the people we are supposed to listen to about cyber security.

A recent Bloomberg News article makes it clear that this was not an isolated incident. It describes how hackers linked to China's army have been seen on the networks of a vast array of American businesses. The article describes how what started as assaults on military and defense contractors have widened into a rash of attacks from which no corporate entity is safe. Among other cyber attacks, Bloomberg News reported, the networks of major oil companies have been harvested for seismic maps charting oil reserves—it saves work if you can steal that information rather than find it yourself—

patent law firms have been hacked for their clients' trade secrets—again, free access to valuable information—and investment banks have been hacked into for market analysis that might impact the global ventures of certain state-owned—nation-state-owned, foreign-country-owned operations.

After having been victimized repeatedly by cyber attacks and having learned about them only when the government arrived to help them fix the problem, one would think critical infrastructure operators or their representatives would be keenly aware of the urgent need for cyber security legislation. One would think they might come to this issue with some sense of humility based on the patent inadequacy of their defenses. One would think that elected officials sworn to the protection of this country might view with some caution and some skepticism claims by folks who are hacked and penetrated virtually at will, usually without even knowing about it, that they can handle this just fine on their own. Yet industry opposition remains, even after the bill has been revised to include a very business-friendly, voluntary, incentive-based approach to hardening up critical infrastructure that we all depend on. Unfortunately, some colleagues can only hear the siren song of the industry lobbyists, even with plain and ominous national security threats staring them in the face.

Some in industry claim that a bill with only information sharing between the government and business would be sufficient and that protection of critical infrastructure is not necessary. This premise is wrong. Statements to the contrary are simply false. Such assertions have been repudiated by the people who lead the charge with our Nation's defense, and who have been confirmed in these roles by the Senate who have repeatedly, and as recently as today, emphasized the need to protect critical infrastructure. These officials include Secretary of Defense Panetta, Director of National Intelligence Clapper, Attorney General Holder, Secretary of Homeland Security Napolitano, and others.

Indeed, it is not just this administration that holds this view. A wide range of national security experts from previous Republican administrations have emphasized the vulnerability of our critical infrastructure, including former Director of National Intelligence and NSA Director ADM Mike McConnell, former Secretary of Homeland Security Michael Chertoff, and former assistant attorney general OLC, and now Harvard Law School professor Jack Goldsmith. These people know what they are talking about, they are not kidding around, and they deserve to be listened to.

Secretary Chertoff has explained that the existing status quo is not generating adequate cyber security for our critical infrastructure. The marketplace, former Homeland Security Secretary Chertoff has explained, is likely to fail in allocating the correct amount of investment to manage risk across the breadth of the networks on which our society relies. One example of this type of market failure is the decision of gas, electric power, and water utility industries to forgo implementation of a powerful new encryption system to shield substations, pipeline compressors, and other key infrastructure from cyber attack because of cost concerns. It should be noted the costs in this case would be approximately $500 per vulnerable device, and they still would not do it.

The unwillingness of industry to adopt necessary security standards is particularly troubling when we consider the scope and scale of the risks associated with a failure of critical infrastructure. The current electricity grid knocked down in India—leaving 600 million people without power—shows how bad things can get when critical infrastructure fails. The cause of this massive failure is not clear, and there is not yet any evidence that it was caused by a cyber attack, but it vividly illustrates the vulnerability of humankind when the critical infrastructure we depend on is knocked down and of the terrible possible consequences of the failure of that critical infrastructure.

The scale of the threat we face, the plain inadequacy of current safeguards in the corporate sector, and the consequences of failure in this area of critical infrastructure all join together to demand passage of comprehensive cyber security legislation. This is a matter of national security. It is our responsibility here in this building to do what we can to make the Nation safer regardless of any parochial interests. Now is the time for us all to come together to get this important job done.

I will conclude by saying we are tantalizingly close to having an agreement. If people will take one last step forward to get that agreement, I think we can do it. If people back away because of the urging of parochial interests, we will fail at this opportunity.

I want to conclude by expressing my congratulations to the chairman of the committee on Homeland Security and his ranking member who have worked hard and who have given an enormous amount. We began with a traditional government-run regulatory procedure, which is one that everybody is familiar with and has lots of checks and balances in it, but it is also a fairly mandatory and top-controlled procedure. As a result of considerable bipartisan discussions, a new model emerged that allows the industry immense independence and control in this area.

The regime it has been moved to is a huge step by the chairman and the ranking member and begins with the rule that originates in the private sector, has it vetted by experts from the private sector, has a national institute for science and technology review as well, ends up with an array of government agencies approving or disapproving that, and whatever standard is ultimately approved by the government council of agencies, the industry companies are free to opt in or opt out. If they think the regulation is unreasonable, they are at liberty to opt out entirely. A comprehensive liability protection structure has been created as an inducement for companies to participate, but it is a strong and powerful check on the standard-setting apparatus that ultimately the industry can choose to opt out if it is unreasonable. An enormous step has been taken by the authors of the current bill toward a compromise. We need a step coming back the other way in order to get this done.

I see my distinguished colleague from Tennessee is here. Let me take one moment as I yield to express my appreciation to Nick Patterson of the Department of Justice who has been on my staff on assignment from the national security division for months and months working on this issue. Today is his last day. I want to thank him for his work on this effort. I want to thank the Department of Justice for loaning him to me and having them lose this valuable member of their national security division to help us develop this legislation. He has been a valuable part of an immensely capable team in my office, led by Stephen Lilley, that has gotten us to at least where I am today on this legislation.

I thank the Presiding Officer, and I thank the Senator from Tennessee for his courtesy.

I yield the floor.

The PRESIDING OFFICER. The Senator from Tennessee.

Mr. ALEXANDER. Mr. President, the majority leader is coming to the floor at 6:30, and I will yield to him at that time.

I would like to thank Neena Imam, who is sitting with me, for serving on my staff for the past two years as a fellow with the Oak Ridge National Laboratory. She has done a terrific job working for me on energy and environmental policy.

Mr. President, today is the 100th anniversary of Milton Friedman's birthday, the Nobel Prize Laureate. One of his most important statements, in my opinion, was this, ''Nothing is so permanent as a temporary government program.'' It was reported by several media outlets that Governor Mitt Romney has taken the position that the wind production tax credit should be allowed to expire at the end of the year. He must have known Milton Friedman's birthday was coming today. I wouldn't presume to speak for Milton Friedman, but I think he would applaud Governor Romney's position. It shows his seriousness about our fiscal problems in the United States. It's time to end a temporary tax credit that was put into law in 1992, when President George H.W. Bush was in office and when Milton Friedman was

only 80 years old. The wind production tax credit was a temporary tax break, in 1992 to encourage wind power. We give wind developers 2.2 cents for every kilowatt-hour of wind electricity produced. And now it's about to expire at the end of the year. It needs to be extended again the developers say. Nothing is so permanent as a temporary government program. They tell us just one more time. But it is an argument like this that has got us into the fiscal mess we have as a Nation.

The United States of America, according to the Joint Tax Committee and the U.S. Treasury, is spending $14 billion on subsidizing giant wind turbines over a five-year period, $6 billion of it is this production tax credit. That's why I am so pleased to see Governor Romney support the idea of more responsibility in our spending. We spend too much money in Washington that we do not have, and it has to stop. There are many reasons we don't need this particular provision of the tax code.

First, we can't afford it. From 2009 through 2013, the tax credit will cost taxpayers $6 billion over five years, and the grants will cost another $8 billion over that same five years. At a time when the federal government is borrowing 40 cents of every dollar it spends, we cannot justify such a subsidy, especially for what the U.S. Energy Secretary calls a ''mature technology.''

Second, despite all the money, it produces a relatively small amount of electricity, producing only 2.3 percent of our electricity in the United States. We're a big country. We use 25 percent of all the electricity in the world. We're not going to operate our country through windmills.

Third, these massive turbines too often destroy the environment in the name of saving the environment. Some are 50 stories high—taller than the Statue of Liberty—with blades as long as a football field, weighing seven tons and spinning at 150 miles an hour, with blinking lights visible for 20 miles. These aren't your grandma's windmills. These gigantic turbines are three times as tall as the sky boxes at University of Tennessee's Neyland Stadium in Knoxville. There is a new movie called ''Windfall'' about residents in upstate New York who are upset and have left their homes because of these big wind turbines.

Mr. President, the majority leader has come to the floor, and I will forgo my remarks at this time so he has a chance to say what he wishes to say.

Mr. REID. Mr. President, it is my understanding that the senior Senator from Tennessee wishes to speak for another 10 minutes, is that right?

Mr. ALEXANDER. Mr. President, 5 minutes would do it.

Mr. REID. Mr. President, I ask unanimous consent that the period for debate only on S. 3414, the Cybersecurity Act of 2012, be extended until 6:40, and that at 6:40 I be recognized.

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

The Senator from Tennessee.

Mr. ALEXANDER. I thank the majority leader for his courtesy, and I will continue.

The fourth reason that we don't need to allow these production tax credits for wind to be renewed is that they have not created as many American jobs as expected. An American University study reported in 2009 that the first $1 billion of stimulus grants to wind went to foreign manufacturing companies.

And what did we get in return for these billions of dollars of subsidies? A puny amount of unreliable electricity generated mostly at night when we don't use it.

I mentioned a little earlier that our country is a big country. It uses lots of electricity. The Senator from Rhode Island was talking about the problems in India that are being caused by failure of the grid. We need large amounts of reliable baseload electricity to power this country. We're very fortunate that we have, through unconventional natural gas discoveries, found that we're going to have a lot of cheap natural gas in the United States, and we can make electricity from natural gas power plants at a low cost and with very little air pollution.

Nuclear power produces 70 percent of our carbon-free electricity, and 20 percent of the total electricity generated in the U.S. It needs to be a part of our future energy mix. Coal should also be part of our energy future, as long as coal plants have pollution control equipment on them to reduce the sulfur, nitrogen and mercury. I was one of those senators who voted to require coal plants that operate in the future to have pollution control equipment on them. This means in a few years every operating coal plant in the United States will be clean except for carbon, and I am convinced that such programs as ARPA-E at the Department of Energy will find what I think is the holy grail of energy technologies.

One of the companies that ARPA-E invests federal research dollars in is experimenting with growing micro-organisms on electrodes. These bacteria can turn carbon dioxide into fuel. In other words, they create a commercial energy use for the carbon that comes from our coal plants. And when that happens, the United States will have massive amounts of cheap, clean, reliable electricity. And we won't be powering our country with windmills.

We should congratulate Dr. Friedman for his great career, for his wisdom in pointing out to us that nothing is so permanent as a temporary government program, and applaud Governor Romney for recognizing that and calling for the end of this tax credit.

We're coming upon something we call the fiscal cliff. I know the senator from Colorado is very interested in this, spending a lot of time working in a bipartisan way to try to find a way to deal with it. My friend, the Foreign Minister of Australia, is a great fan of the United States, and he said to the United States that we're one budget agreement away from restoring our global preeminence—One budget agreement away from restoring our global preeminence.

Now, to get that agreement what do we have to do? We have to deal with appropriations bills at the end of the year, a problem we may have solved today with a solution the leaders recommended. We have to deal with the Bush tax cuts, and multiple items that expire at the end of the year such as the tax extenders that need to be renewed or not, and the alternative minimum tax which started out as a tax on rich people and now threatens to impact millions of Americans. There's appropriate payment to doctors who provide medical care, we call this the doc fix. There is the sequester that none of us likes. There's the problem of the debt limit, the payroll tax cut and unemployment benefits. All of this is happening at the end of the year.

This is a good time to get serious about with dealing with the fiscal cliff, and let a 20 year, temporary tax break to encourage wind energy—which costs the American people $6 billion over five years—to expire and let wind stand on its own. I would suggest that for the $6 billion in savings we put $2 of every $3 we save into reducing the debt and $1 into energy research to see if we can find even more amounts of cheap, clean energy.

So it is a good occasion to celebrate Milton Friedman's 100th birthday, and it is a good occasion to applaud Governor Romney for following Milton Friedman's advice: ''Nothing is so permanent as a temporary government program.''

I thank the Presiding Officer. I thank the majority leader for his courtesy.

Mr. WHITEHOUSE. Mr. President, I rise to discuss three amendments to the Cybersecurity Act of 2012 that I am introducing today with Senator MIKULSKI. This important piece of legislation, which was introduced by Senators LIEBERMAN, COLLINS, FEINSTEIN, ROCKEFELLER, and CARPER, responds to the serious and growing cyber security threat facing our Nation. It will strengthen our national security, our economic well-being, the safety of our families, and our privacy. The three amendments Senator MIKULSKI and I are introducing today would ensure that the bill also harnesses law enforcement agencies' cyber authorities and capabilities as effectively as possible.

I am very honored that Senator MIKULSKI is introducing these amendments with me today. She has a long record of continued leadership on law enforcement and national security issues. It has been a privilege to work with her on the challenge of protecting Americans against cyber security threats, first on the Intelligence Committee and more recently in a series of

discussion and working groups. As the chairman for the Commerce, Justice, Science, and Related Agencies Subcommittee of the Appropriations Committee, her assessment of the right approach to law enforcement issues in cyberspace draws from a wealth of experience and expertise. I am very grateful to her for her leadership on these issues.

The first amendment we have introduced addresses the scale and structure of law enforcement's cyber resources. Law enforcement agencies have vital roles to play against cyber crime, cyber espionage, and other emerging and growing cyber threats. Congress must ensure that law enforcement agencies are organized and resourced in a manner that allows them to fulfill these important responsibilities. To date, investigatory responsibilities for cyber crime have been assigned within existing agencies, with some held by the FBI and others by the Secret Service or other agencies. Prosecutorial responsibilities have been distributed among the National Security Division, the Computer Crime and Intellectual Property Section, and U.S. attorneys' offices across the country. Law enforcement has had some important successes with this model, such as the FBI's takedown of the Coreflood botnet, but these successes need to be achieved with much greater frequency.

FBI Director Mueller stated that a ''substantial reorientation of the Bureau'' will be necessary to achieve that goal. It is Congress's responsibility to ensure that any reorientation of law enforcement maximizes law enforcement's effectiveness against the cyber threat and uses Federal resources as efficiently as possible. This will require Congress to consider important issues such as whether cyber crime should have a dedicated investigatory agency akin to the DEA or ATF, whether existing task force or strike force models are well suited for addressing the cyber threat, and how cyber resources should be scaled given the future threat.

To address these questions, our amendment would require an expert study of our current cyber law enforcement resources. This study will evaluate the scale and structure of these resources, identifying strengths and weaknesses in the current approach and providing recommendations for the future. This amendment thus will provide Congress a necessary expert assessment to guide our work in the years ahead.

The second amendment we have introduced would ensure that existing and effective cyber law enforcements efforts are not unintentionally disrupted by changes made in title II of the bill, which covers ''Federal Information Security Management and Consolidating Resources.'' This title makes a number of valuable changes and reforms to current law, including the creation of a center within the Department of Homeland Security that will lead efforts to protect Federal Government networks. The creation of this center is an important step forward in protecting Federal networks, but we must ensure that its operations do not disrupt law enforcement relationships and activities that currently are making our country safer. For example, the FBI-led National Cyber Investigative Joint Task Force, NCIJTF, must be allowed to continue its much needed and effective work on cyber law enforcement and intelligence.

Our amendment would clarify that the new center is focused on the protection of Federal networks and that its responsibilities do not extend to law enforcement. Specifically, the amendment would add a savings clause indicating that the title does not pertain to law enforcement or intelligence activities. It also would add definitions that help provide a clearer picture of the new center's role in protecting Federal Government networks and responding to cyber threats, vulnerabilities, or incidents.

The final amendment we are introducing today is to title VI, which covers international cooperation. This title, which incorporates legislation first introduced by Senator GILLIBRAND and Senator HATCH, will help clarify and strengthen the ability of the Federal Government and particularly the Department of State to develop international cyber security policy. Language in the title, however, could be read to disrupt existing and effective working relationships between American and foreign law enforcement agencies, interfere with the exercise of prosecutorial discretion, and to limit the Department of Justice's accountability to Congress for the law enforcement decisions it makes. Our amendment would ensure that the Department of Justice works collaboratively with the Department of State as it exercises its prosecutorial discretion and that it is accountable to Congress for cyber crime issues for which it is responsible and regarding which it has particular expertise.

I look forward to working with the managers of S. 3414 and any interested colleagues on these important issues. I thank Senator MIKULSKI for her cosponsorship.

I yield the floor, and I note the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

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

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

Mr. REID. Mr. President, to say I am disappointed is a tremendous understatement. This body is debating a measure that would prevent what national security experts on a bipartisan basis have called a serious threat to our Nation since the dawn of the nuclear age. Senator MCCAIN called this danger an existential threat to our Nation.

Democrats were prepared to work on a bipartisan basis to pass this legislation. I, personally, have convened many meetings, going back 2 years ago, to have a piece of legislation that we could pass through this body. In that 2 years' time, things have gotten worse, not better, as far as threats to our country. We have been prepared to address concerns raised by the private sector, and I think it is only fair to say that for the leaders of the committees involved in this issue, there has been real cooperation, from both Democrats and Republicans.

I have said on the Senate floor many times that the work of Senator LIEBERMAN and Senator COLLINS has been exemplary. The major part of this bill is within their jurisdiction dealing with homeland security. I have always envisioned they have been prepared to engage in a robust debate and to consider amendments designed to perfect the bill. I know that is how I feel. Above all, I thought we had all been prepared to put national security above partisan politics to address this urgent matter.

I was surprised this morning to hear Senator MCCONNELL say he would like a vote on repealing ObamaCare on this bill. That is really not appropriate. Some Republican Senators have said this matter is going to be filibustered unless they have the right to vote on an amendment to repeal health care reform. Obviously, that is it. The Republican leader said that, but then I thought that might fade away.

Every Tuesday after our caucuses—the Republicans have one and the Democrats have one—Senator MCCONNELL and I meet at the Ohio clock, as it is called, and both of us make a statement and answer questions the press gives us. It is not a jump ball, as in whoever gets there first gets to make the first presentation. We wait, and if one of us is not ready, the other goes first.

Sometimes he goes first; sometimes I go first. But the important point in the one today is that—and I am paraphrasing but the point is certainly valid—the Republican leader said out here, with the entire press corps and his leadership team with him, that cyber security—remember, I am paraphrasing—is something we should do, but it will take several weeks to do it. Not this week.

Compare that to the words of GEN Keith Alexander, commander of the U.S. Cyber Command, who wrote Senator MCCONNELL and I today. And here is what he said. This is a quote:

> The cyber threat facing this Nation is real and demands immediate action. The time to act is now. We simply cannot afford further delay.

I have tried to figure out a way of describing how I feel about this. I said ''disappointed,'' and that is certainly true; ''flummoxed,'' that is certainly true. I cannot understand why we are in this position. I am so disappointed that Leader MCCONNELL and his colleagues—some of his colleagues—would

prevent us from acting on this urgent threat. I am particularly astounded they would rather launch yet another attack, for example, on women's health than work to ensure the security of our Nation.

I have no choice but to file cloture on this matter. I would hope we could get cloture, but I am a realist, as I have learned after having tried to work through 85 different filibusters in this congressional session. I remain hopeful that they will come to their senses and realize the urgent need for action on this matter.

There was a really inspirational presentation made in our caucus today by Senator BARBARA MIKULSKI of Maryland. Again, I am paraphrasing, but I am pretty direct in remembering what she said. I was not present when Senator MCCONNELL made his statement. Senator MIKULSKI said: I have served on the Intelligence Committee for 10 years. And she said: This legislation creates a rendezvous with destiny for our country. We have to do something, and we have to do it soon.

I have stated to Senator LIEBERMAN, to Senator COLLINS—anyone who will listen—this is not a partisan piece of legislation. It should not be. I am happy to work on an agreement to consider relevant amendments, but this matter has been pending since last Thursday. Today is Tuesday, and basically the slow walk that I am so used to around here has taken place.

I hope we can find a final path forward. Senators from both sides of the aisle have come to me personally and said they have invested time—lots of time—in this matter, and they are trying to forge a consensus. I take them at their word, but they all seem powerless to buck the filibuster trend we have.

So I hope when the dust settles we can set aside crass politics and work together for the good of our Nation and can achieve a strong, effective, bipartisan cyber security bill.

Mr. President, Tom Donohue, head of the Chamber of Commerce, is my friend. He really is. But I am terribly disappointed in the Chamber of Commerce. We started out with having a requirement that businesses in the private sector would be required to do certain things. Senators LIEBERMAN and COLLINS backed off from that, and now it is kind of a voluntary deal. It is much weaker than I think it should be. Why in the world would they oppose that—''they'' meaning the Chamber of Commerce, which has sucked in most all of the Republicans on this. That is really unfortunate.

AMENDMENT NO. 2731

So, Mr. President, on behalf of Senators LIEBERMAN, COLLINS, and others, I call up amendment No. 2731, which is at the desk.

The PRESIDING OFFICER. The clerk will report.

The bill clerk read as follows:

The Senator from Nevada [Mr. REID], for Mr. LIEBERMAN, for himself, Ms. COLLINS, Mr. ROCKEFELLER, Mrs. FEINSTEIN, and Mr. CARPER, proposes an amendment numbered 2731.

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

Mr. REID. Mr. President, I ask for the yeas and nays on that amendment.

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The yeas and nays were ordered.

AMENDMENT NO. 2732 TO AMENDMENT NO. 2731

Mr. REID. Mr. President, on behalf of Senator FRANKEN, I call up amendment No. 2732, which is also at the desk.

The PRESIDING OFFICER. The clerk will report.

The bill clerk read as follows:

The Senator from Nevada [Mr. REID], for Mr. FRANKEN, proposes an amendment numbered 2732 to amendment No. 2731.

The amendment is as follows:

At the end, add the following new section:

SEC. ___.

Notwithstanding any other provision of this Act, section 701 and section 706(a)(1) shall have no effect.

AMENDMENT NO. 2733

Mr. REID. Mr. President, I have an amendment to the language proposed to be stricken.

The PRESIDING OFFICER. The clerk will report.

The bill clerk read as follows:

The Senator from Nevada [Mr. REID] proposes an amendment numbered 2733 to the language proposed to be stricken by amendment No. 2731.

The amendment is as follows:

On page 20, line 5, strike ''180 days'' and insert ''170 days''.

Mr. REID. Mr. President, I ask for the yeas and nays on that amendment.

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The yeas and nays were ordered.

AMENDMENT NO. 2734 TO AMENDMENT NO. 2733

Mr. REID. Mr. President, I have a second-degree amendment at the desk.

The PRESIDING OFFICER. The clerk will report.

The bill clerk read as follows:

The Senator from Nevada [Mr. REID] proposes an amendment numbered 2734 to amendment No. 2733.

The amendment is as follows:

In the amendment strike ''170'' and insert ''160''.

CLOTURE MOTION

Mr. REID. Mr. President, I have a cloture motion at the desk.

The PRESIDING OFFICER. The cloture motion having been presented under rule XXII, the Chair directs the clerk to read the motion.

The bill clerk read as follows:

CLOTURE MOTION

We, the undersigned Senators, in accordance with the provisions of rule XXII of the Standing Rules of the Senate, hereby move to bring to a close debate on S. 3414, a bill to enhance the security and resiliency of the cyber and communications infrastructure of the United States.

Harry Reid, Joseph I. Lieberman, Barbara A. Mikulski, Thomas R. Carper, Richard J. Durbin, Christopher A. Coons, Mark Udall, Ben Nelson, Jeanne Shaheen, Tom Udall, Daniel K. Inouye, Carl Levin, John D. Rockefeller IV, Charles E. Schumer, Sheldon Whitehouse, John F. Kerry, Michael F. Bennet.

MOTION TO COMMIT WITH AMENDMENT NO. 2735

Mr. REID. Mr. President, I have a motion to commit the bill with instructions, which is at the desk.

The PRESIDING OFFICER. The clerk will report the motion.

The bill clerk read as follows:

The Senator from Nevada [Mr. REID] moves to commit the bill, S. 3414, to the Committee on Homeland Security and Governmental Affairs with instructions to report back forthwith with an amendment numbered 2735.

The amendment is as follows:

At the end, add the following new section:

SEC. _____.

This Act shall become effective 3 days after enactment.

Mr. REID. Mr. President, I ask for the yeas and nays on that motion.

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The yeas and nays were ordered.

AMENDMENT NO. 2736

Mr. REID. Mr. President, I have an amendment to the instructions at the desk.

The PRESIDING OFFICER. The clerk will report.

The bill clerk read as follows:

The Senator from Nevada [Mr. REID] proposes an amendment numbered 2736 to the instructions (amendment No. 2735) of the motion to commit S. 3414.

The amendment is as follows:

In the amendment, strike ''3 days'' and insert ''2 days''.

Mr. REID. I ask for the yeas and nays on that amendment.

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The yeas and nays were ordered.

AMENDMENT NO. 2737 TO AMENDMENT NO. 2736

Mr. REID. Mr. President, I have a second-degree amendment at the desk.

The PRESIDING OFFICER. The clerk will report.

The bill clerk read as follows:

The Senator from Nevada [Mr. REID] proposes an amendment No. 2737 to amendment No. 2736.

The amendment is as follows:

In the amendment, strike ''2 days'' and insert ''1 day''.

Mr. REID. Mr. President, I ask unanimous consent that the mandatory quorum required under rule XXII be waived with respect to the cloture motion that has just been filed.

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

VETERANS JOBS CORPS ACT OF 2012—MOTION TO PROCEED

Mr. REID. Mr. President, I now move to proceed to Calendar No. 473, S. 3429

The PRESIDING OFFICER. The clerk will report the motion.

The bill clerk read as follows:

Motion to proceed to Calendar No. 473, S. 3429, a bill to require the Secretary of Veterans Affairs to establish a veterans jobs corps, and for other purposes.

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

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. LIEBERMAN. 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 LEGISLATION

Mr. LIEBERMAN. Mr. President, I rise to respond to the statement of the majority leader—first, to say that I share his sadness and disappointment that he had to file a cloture motion on this Cybersecurity Act, but I totally agree with the decision he has made. I do not think he had any choice.

I think we are facing on the one hand an urgent, real, and growing threat to our security and our prosperity because we are vulnerable; that is, the privately owned cyber infrastructure of our country is vulnerable to attack from foreign enemies, from nonstate actors such as terrorist groups, from organized criminal gangs who are just out to steal billions of dollars over the Internet, and from hackers.

So we are dealing with a real problem that all the nonpolitical security experts from the last administration, the Bush administration, and this one, the Obama administration, say is rising rapidly to being the No. 1 threat to American security. Over the Internet now, because of our vulnerability over cyber space, a foreign enemy can do us more damage than the terrorists did to us on 9/11. It is that stark. So that is one reality.

The other reality is that Senator COLLINS and I, Senator ROCKEFELLER and Senator FEINSTEIN, have been working literally for years. As Senator REID said, because of the urgency of the problem, we decided we cannot just fight for 100 percent of what we thought was best to protect our security. We pulled back; we made it not mandatory. We have standards being set for the private sector to defend itself and us better, and we are creating carrots and not sticks to encourage them to opt into those cyber security standards. That is one reality.

The other reality is that in our government—notwithstanding controversy here—all the Departments are working like a team. As General Alexander, the head of Cyber Command at the Department of Defense says, cyber security is a team sport—the Department of Homeland Security, the Department of Defense, the FBI, the intelligence community all working together to protect our country. But they do not have the tools they need, and they urgently need this bill.

Yet the other reality is, in the Senate, where once again we are gridlocked, we cannot even get the consent necessary to take up amendments to vote on. Senator COLLINS and I have said all along: Just get this bill to the floor. Let the Chamber, the 100 Senators, work their will on germane and relevant amendments, and something good will result for the country. So here is the bill on the Senate floor, and yet Members are blocking us from taking up those amendments. And I am afraid the consequence is that they are running out the clock.

A lot of good work done by those of us who have sponsored the pending legislation, in a very constructive, bipartisan group, led by Senator KYL and Senator WHITEHOUSE—including three additional members of the Democratic Caucus and Republican Caucus—have worked very hard to bridge the gaps. We have come closer together, but we are not going to work this out unless we can vote.

I wish we had not come to this point, but Senator REID has made the correct and necessary decision, and it will confront the Members of the Senate on Thursday with a decision: Are you going to vote for cloture to at least allow the Chamber to consider all the amendments on this bill that are germane and relevant or are you going to say: No, I will only settle for exactly what I want, and I do not want this bill; therefore, I am going to vote against cloture and run the risk—which all the independent cyber security experts in our Nation tell us we will run if we do not do anything—that we will suffer a major attack or at least we will continue to suffer major cyber theft.

So I am saddened. We have worked very hard on this. But that is not the point. The point is, there is an urgent necessity to pass this legislation. It ought to be nonpartisan. It ought not to be the victim of special interest pleading. It ought to be all of us coming together, as we usually have on national security matters, to put the national security interests of the American people ahead of special interests, to resolve our differences, to settle for less than 100 percent, and to get something done to protect our country or is this going to be another case where the Senate fails to bridge the gaps, fails to be willing to make principled compromises and therefore fails not only to fix a problem but, in this case, to protect our country from a very clear and present danger of cyber attack and cyber theft?

So Thursday will be the day of decision. I hope perhaps meetings can occur tomorrow in which we can reconcile our differences and agree on a method to go forward. If not, every Member of the Senate is going to have to decide whether they want to block action on cyber security legislation or whether they want to go forward and consider the amendments on both sides that have been filed.

I thank the Presiding Officer and yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

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

The PRESIDING OFFICER (Mr. UDALL of Colorado.) Without objection, it is so ordered.

Mr. LIEBERMAN. Mr. President, it strikes me, as I call you, Mr. President, that I once had the high honor to support a man who shared your name, indeed your father, for President of the United States. So it is nice to be able to call you Mr. President.

MORNING BUSINESS

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the Senate proceed to 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 NED MOORE

Mr. MCCONNELL. Mr. President, I rise to pay tribute to an honored Kentuckian and veteran of World War II, Mr. Ned Moore. Mr. Moore visited the Nation's capital several months ago with Honor Flight, the group that helps bring veterans to Washington, D.C., to see the memorials that were built in their honor. Mr. Moore was able to see the World War II Memorial that he and his fellow sailors inspired.

Ned's grandson, Mr. Tres Watson, is a good friend of mine, and when he made me aware of his grandfather's visit, I thought it worth a moment to share Ned's story with my colleagues. Ned Moore was born in Marydell, MS, on February 27, 1927. He joined the Navy in Jackson, MS, on August 1, 1944, at the age of 16, without his mother's consent. He was assigned to the USS *Coronis*, a landing-craft repair ship, on Christmas Day 1944.

While Ned was aboard the *Coronis*, it saw action throughout the Pacific Theater, including acting as a support ship during the battle of Okinawa.

In 1945, Ned was assigned to the United Nations, where among his duties he served as personal driver for UN delegates including Eleanor Roosevelt, who was a UN delegate at the time. She presented Ned with a Roosevelt dime after making his acquaintance.

In March 1946, Ned was assigned to the USS *Wright*, a *Saipan*-class light aircraft carrier, where he served as an aircraft mechanic. While the *Wright* was stationed in Pensacola, FL, functioning as a training ship, Ned married Margaret Daly in 1948.

In October 1952, Ned was assigned to the USS *Bennington*, an *Essex*-class aircraft carrier that had been

recomissioned as an attack carrier. While the *Bennington* was stationed in Guantanamo Bay, Cuba, in February 1953, then-U.S. Senator John F. Kennedy obtained leave for Ned to return to the United States for the birth of his first child.

In 1958, Ned was assigned to the USS *Wasp* in Boston after it had been overhauled to become the hub of a special anti-submarine group of the Sixth Fleet. While aboard the *Wasp*, Ned sailed through the Mediterranean and participated in Operation Blue Bat, a U.S. military intervention into Lebanon. The *Wasp* was responsible for transporting sick and injured Marines from Lebanon so they could receive care.

In 1960, Ned was transferred to NAS, Naval Air Station Memphis. While in Memphis, Ned established the Naval Air Maintenance Training Group Library. He was also a courier between Memphis and Washington, carrying plans for jets under design.

He retired from the Navy in Memphis on December 31, 1964, as a senior chief petty officer.

After leaving the Navy, Ned and his family moved to Mayfield, KY, where he worked as a maintenance manager at the General Tire manufacturing facility. There, he raised three children, Debbie, Richy, and Mike. After retiring from General Tire in 1983, Ned and his wife kept their house in Mayfield while traveling the country in a motor home in the spring, summer, and fall and wintering in Florida. They travelled to all 50 States. They moved to Lillian, AL, in 2005.

At this time I ask my U.S. Senate colleagues to join me in honoring Mr. Ned Moore for his service to country and his devotion to the defense of freedom. When World War II ended, he laid down his arms to become a productive, successful member of the community who was admired by his family, neighbors, and State. He has been a role model to Tres Watson and many other Kentuckians. I wish him all the best in his retirement and a happy future.

WOOL TRUST FUND

Mr. SCHUMER. Mr. President, I am happy to hear there is a commitment to pass the extension and modification of the Wool and Cotton Trust Funds this year. As my colleagues noted, the Wool Trust Fund compensates for the competitive damage caused by the fact that duties are higher on imports of raw materials, like wool fabric, than on imports of finished products, like trousers and suits. This ''tariff inversion'' gives foreign manufacturers a significant cost advantage over U.S. manufacturers like Rochester, NY's Hickey Freeman.

Hickey Freeman has been operating in Rochester, NY since 1899. Wool cloth imported by Hickey Freeman is cut and sewn into wool clothing which, in turn, is sold in stores across the United States and around the world. I am particularly proud to note—while our athlete's uniforms sadly were made in China, our announcers on NBC are wearing Hickey Freeman at the 2012 London Olympic Games.

The Wool Trust Fund is a successful program in curbing job losses and allowing American textile and apparel companies to expand their own export markets. Without the technical fix that we are asking for here today, the health of the Wool Trust Fund will be in peril.

I thank Senator MENENDEZ for his tireless leadership in extending and modifying the Wool and Cotton Trust Funds and the Leader and Chairman BAUCUS for agreeing to work with Senators MENENDEZ, CARDIN and myself to ensure these important programs are dealt with by the end of the year.

6-MONTH CONTINUING RESOLUTION

Mr. COCHRAN. Mr. President, agreeing to put the government on autopilot for 6 months is no great achievement. It simply means more drift. It means a longer period of uncertainty for government agencies and the people they serve, more spending on ineffective programs and outdated priorities, and inadequate investment in programs that merit additional resources.

My preference is that we complete our work and make specific spending choices based on the relative merits of government programs. There is no excuse for the Senate not to be considering the appropriations bills. Our committee members have done the work of scrutinizing budgets, holding hearings, and drafting bills. Those bills deserve to be considered by the Senate, negotiated with the House and sent to the President as soon as possible.

I congratulate the distinguished chairman of our Committee on Appropriations, Mr. INOUYE, for his dependable leadership on getting us to this point. I look forward to continuing our efforts to extend our appropriations authority for the balance of the fiscal year.

WEAR AMERICAN ACT OF 2012

Mr. BROWN of Ohio. Mr. President, in cities and towns across the Nation, workers have the proud tradition of manufacturing products that are made here at home.

Manufacturing helped us become an economic superpower and build a strong, vibrant middle class.

Ohio manufacturers and workers are some of the most industrious, innovative, and competitive in the Nation.

Our companies and the hard-working people who fill our factories can compete with anyone in the world.

But this competition is getting tougher as our Nation is facing ongoing and unfair competition from countries like China.

It does not help when U.S. companies and organizations either outsource jobs, production, and purchases overseas.

As has been reported in the news recently, the U.S. Olympic Committee's use of Chinese-made apparel was a missed opportunity to use domestic apparel manufacturers.

The public outrage about this decision created was predictable.

It is unconscionable that the U.S. Olympic Committee would hand over the production of uniforms worn by our proud athletes to a county that flouts international trade laws, manipulates its currency, and cheats on trade.

It makes no sense that an American organization would place a Chinese-made beret on the heads of our finest athletes when we have the capacity to make high-end apparel here.

I am encouraged that, after speaking with the chief executive and chair of the U.S. Olympic Committee, uniforms designed by Ralph Lauren for the 2014 Olympic Games will be made in the United States.

I also applaud USOC's decision to further ensure, as a matter of policy, that they are going to make Buying American a priority.

But this incident reminds us of the consequences of passing a trade deal without real accountability and enforcement.

Congress passed a trade deal with China more than 10 years ago, which has contributed to the loss of more than 5 million U.S. manufacturing jobs between 2000 and 2010.

While some lawmakers and economists have written off our manufacturing sector including textile and apparel production they need to think again.

According to the National Council of Textile Organizations, the United States is the third largest exporter of textile products in the world.

The textile sector put more than 500,000 people to work at plants in large cities and mills in rural towns.

Do some lawmakers and economists really think we should turn our backs these working Americans?

No. It is not right that U.S. workers get overlooked when it comes to showcasing that American apparel workers in Ohio towns like Brooklyn and Aracanum can make things.

We've seen this time and time again: whether it is Olympic uniforms or U.S. flags, products all too often are not made here.

We can and we must stop this disturbing trend.

That is why I am introducing the Wear American Act to make certain that the Federal Government purchases apparel that is 100 percent American-made.

That means all textiles and apparel purchased with U.S. tax dollars will be invested in U.S. businesses and communities not China.

The textile industry has been a staple of our Nation's economy since its founding and it will be important in the future.

The United States is the world leader in textile research and development.

American companies and universities are developing new textile materials such as conductive fabric with antistatic properties and high-tech textiles that monitor movement and heart rates.

When consumers in the United States and around the world demand our products, we deliver.

The United States textile industry is the third leading exporter of products worldwide. In fact, recently total textile and apparel exports reached a record $22.4 billion.

This legislation makes sense plain and clear. Why shouldn't our national policies support American companies and workers?

We should be in the business of creating policies that reward hard working Americans who work hard every day rather than supporting a Tax Code and trade policies that help big companies send U.S. jobs overseas.

Right now, the stakes couldn't be higher.

That is why the Wear American Act and supporting American workers is so important.

U.S.-MOROCCO PEACE AND FRIENDSHIP TREATY

Mr. CASEY. Mr. President: I would like to take this occasion to extend congratulations to His Majesty King Mohammed VI and the people of Morocco on the 225th anniversary of the Treaty of Peace and Friendship between the United States and the Kingdom of Morocco.

Negotiations for this treaty began in 1783 and the draft was signed in 1786. Future Presidents John Adams and Thomas Jefferson were the American signatories. The treaty was then presented to the Senate, which ratified it on July 18, 1787, making it the first treaty to receive U.S. Senate ratification.

The treaty represented the second time that Morocco and the United States affirmed diplomatic relations between the two countries. It is also worthy of mention that that Sultan, Mohammed III, was the first head of state, and Morocco the first country, to recognize the new United States as an independent country in 1777.

The Treaty of Peace and Friendship, whose anniversary we commemorate this month, provided for the United States' diplomatic representation in Morocco and open commerce at any Moroccan port on the basis of ''most favored nation.'' It also established the principle of non-hostility when either country was engaged in war with any other nation.

Most importantly, the treaty provided for the protection of U.S. shipping vessels at a time when American merchant ships were at risk of harassment by various European warships. The treaty specifically stated:

If any Vessel belonging to the United States shall be in any of the Ports of His Majesty's Dominions, or within Gunshot of his Forts, she shall he protected as much as possible and no Vessel whatever belonging either to Moorish or Christian Powers with whom the United States may be at War, shall be permitted to follow or engage her, as we now deem the Citizens of America our good Friends.

A further indication of the early and close relationship between the United States and Morocco can be seen in a letter President George Washington wrote to Sultan Mohammed III on December 1, 1789. President Washington wrote:

It gives me pleasure to have this opportunity of assuring your majesty that I shall not cease to promote every measure that may conduce to the friendship and harmony which so happily subsist between your empire and these . . . This young nation, just recovering from the waste and desolation of long war, has not, as yet, had time to acquire riches by agriculture or commerce. But our soil is beautiful, and our people industrious and we have reason to flatter ourselves that we shall gradually become useful to our friends.

United States relations with Morocco have strengthened in the decades and centuries following the historic treaty. For example, during World War I, Morocco was aligned with the Allied forces, and in 1917 and 1918, Moroccan soldiers fought valiantly alongside United States Marines at Chateau Thierry, Mont Blanc, and Soissons.

During World War II, Moroccan national defense forces aided American and British forces in the region. Morocco hosted one of the most pivotal meetings of the Allied leaders in World War II. In January 1943, United States President Franklin Roosevelt, British Prime Minister Winston Churchill and Free French commander Charles De Gaulle met for 4 days in the Casablanca neighborhood of Anfa to discuss strategy against the Axis powers. It was during this series of meetings that the Allies agreed to launch their continental counter push against Axis aggression through a beach head landing on the French Atlantic coast.

Following Morocco's independence in 1956, President Dwight Eisenhower communicated to King Mohammed V that ''my government renews its wishes for the peace and prosperity of Morocco.'' The King responded by reassuring President Eisenhower that Morocco would be a staunch ally in the fight against the proliferation of communism in the region.

The United States Agency for International Development, USAID, and its predecessor agencies, as well as the Peace Corps, have been active in Morocco since 1953. Currently, there are more than 200 volunteers in Morocco working in the areas of health, youth development, small business and the environment.

Following the September 11, 2001 attacks, Morocco was one of the first nations to express its solidarity with the United States and immediately renewed its commitment as a strong ally to combat terrorism. Cooperation between the United States and Morocco on these issues includes data sharing, law enforcement partnerships, improved capabilities to oversee strategic checkpoints, and joint efforts to terminate terrorist organization financing.

It is important to extend our warm congratulations to His Majesty King Mohammed VI as well as to the people of Morocco on the anniversary of the Treaty of Peace and Friendship, which set the stage for continued and sustained engagement between our two countries.

ADDITIONAL STATEMENTS

REMEMBERING JOHN W. MAHAN

• Mr. BAUCUS. Mr. President, today I wish to recognize a remarkable Montanan and American. John W. Mahan, or Jack as we all knew him, died peacefully on Independence Day, July 4, at his home in Helena, MT. He was my neighbor and friend. I ask my colleagues in the Senate to join me in honoring Jack and offering condolences to his family and loved ones.

The Fourth of July was a fitting day for this World War II veteran and lifelong national veterans' advocate to leave this world. Majority leader Mike Mansfield, a veteran of World War I, once said that Jack Mahan ''has done more for the veterans of Montana and the nation than any other man I know.''

Jack was born into a family dedicated to national service. His father, John Senior, served as the national commander of the Disabled American Veterans as a brigadier general. John Senior later served as Montana's adjutant general. Jack's mother Iola served as president of the American Legion Auxiliary in Helena.

After the Japanese attack on Pearl Harbor, Jack enlisted in the Navy Air Corps. Jack went on to bravely serve as a dive bomber pilot in the Pacific during World War II.

After the war, Jack took the lead on tackling challenges facing his fellow World War II veterans in Montana and across the country.

Jack fought for bonuses for WWII veterans—a practice that was done after WWI to help get returning troops back on their feet.

Although, the Montana Supreme Court declared these ''bonus'' payments unconstitutional, Jack worked with veterans groups and Montana officials to build popular support and eventually secured an ''honorarium'' payment instead of a ''bonus.'' Jack's ''honorarium,'' paid for by a 2-cent tax on cigarettes, raised $22 million for World War II veterans. In today's dollars, that is $226 million.

In the late 1950s, Jack led the way in establishing the veterans hospital at Fort Harrison, west of Helena.

Again, Jack worked with Montanans, veterans groups, and Members of Congress to raise $5.4 million to begin the first phase of building for the hospital.

Today, Montana veterans still rely on the hospital in Fort Harrison for their basic medical needs.

During his work, Jack met the acquaintance and earned the respect of Presidents Dwight D. Eisenhower, John F. Kennedy, Lyndon B. Johnson, Richard Nixon, and Gerald Ford.

Jack had a truly remarkable life and career of service to our country. He served as the national commander-in-chief of Veterans of Foreign Wars from 1958 to 1959.

He served as the national chairman of the Veterans for John F. Kennedy's Presidential campaign committee in 1960. He also served as the under secretary to the VA Memorial Services and Director of the National Cemetery System in the Nixon administration.

On this very day, we have brave Americans patrolling the mountains of Afghanistan. May Jack's memory be a reminder of the obligation we owe to these brave warriors when they come home. His legacy is a reminder of what dedicated public service can deliver for our Nation's finest. We will miss you, Jack.●

TRIBUTE TO DES R. GOYAL

● Mr. BLUNT. Mr. President, I rise today to honor Des R. Goyal as he completes a long and distinguished career with the U.S. Army Corps of Engineers, USACE. Mr. Goyal was born and educated in India, where he eventually received his Bachelor's and Master's degrees in Mechanical Engineering. In 1970, he came to the United States to further his studies while earning his U.S. citizenship. Mr. Goyal started his career with the Corps in 1978 as a project engineer on navigation locks in the Corps of Engineers Huntington District. Since that time, he has held numerous assignments with the Corps of Engineers, including working on military construction projects in Saudi Arabia and serving in Germany as Chief of the Mechanical/Electrical design branch for the Corps of Engineers Europe Division. In 1999, he was assigned the job of Chief, Operations Division, Kansas City District of the Corps of Engineers.

2011 was arguably the most challenging year in the 114-plus-year history of the Corps of Engineers, Kansas City District. While executing the challenging Operations and Maintenance program, the District battled an epic 145-day flood in the Missouri River Basin and established a Recovery Field Office in Joplin, MO to respond to the fifth deadliest tornado in U.S. history. As an integral part of the Operations Division, Mr. Goyal led the effort to ensure his Emergency Management and Contingency Operations were fully manned by competent personnel from throughout the District. These additional missions comprised approximately 25 percent of the Kansas City District's workforce at various times, placing significant stress on the organization. However, Mr. Goyal remained poised and calm, responding with a plea for volunteers, and was instrumental in the success of these efforts. During these challenges, he clearly demonstrated strong leadership and technical competency. His past experiences significantly augmented the success of the mission during this timeframe.

Throughout his career, Des Goyal has promoted leadership and mission execution. He has mentored many USACE employees and military personnel while leading the efforts on large, complex projects and programs throughout the world. He has tremendous passion for the advancement of his colleagues and those they serve. He championed the use of the Student Career Employment Program, SCEP, in the Corps of Engineers Northwest District, which serves as a valuable tool in providing college students the critical experience and networking opportunities to encourage employment in a public service career. Mr. Goyal continues to press for positive change through a focus on good government, professional organizations and community service.

I thank Des Goyal for his service to his adopted country and wish Des and his wife, Usha, an enjoyable retirement.●

NORTHWEST KIDNEY CENTERS

● Ms. CANTWELL. Mr. President, today I wish to congratulate Northwest Kidney Centers on its 50th Anniversary. Northwest Kidney Centers was established as the first out-of-hospital dialysis program in the world, opening its doors in Seattle, WA, on January 8, 1962.

Just 2 years after the development of the Teflon shunt at the University of Washington, community leaders in Seattle came together to raise money and find a space to establish a center to deliver dialysis treatments outside of a hospital, which led to the creation of the community-based Northwest Kidney Centers.

Chronic kidney disease is now an epidemic, affecting one in seven American adults. Northwest Kidney Centers is working to reverse this trend, focusing on community education and prevention. Each year, Northwest Kidney Centers allocates funding toward public health education about kidney disease and organ donation, participating in outreach events and reaching more than 12,000 people with kidney information. It also developed a ''Living Well with CKD'' program which offers classes on treatment options and good nutrition. This program reaches nearly 1,000 pre-dialysis patients and family members each year, at no cost to the participants.

I take great pride in the fact that Seattle is the birthplace of chronic dialysis treatments and that Northwest Kidney Centers continues to take the lead on developments in the field. Northwest Kidney Centers hosted clinical trials to develop the anti-anemia drug Epogen, and set up the Northwest Organ Procurement Agency. In 2008, Northwest Kidney Centers spearheaded the creation of the Kidney Research Institute, a collaboration with the University of Washington Medical School which has become a scientific leader focusing on ways to prevent, detect, treat, and eventually cure kidney disease.

I applaud Northwest Kidney Centers for its contributions to the State of Washington and the kidney disease and dialysis field as a whole. As the organization celebrates its 50th Anniversary, I extend my congratulations to the entire Northwest Kidney Centers community—patients, physicians, employees, supporters and volunteers—and thank them for their dedication and commitment to improving the lives of kidney patients in my State.●

RECOGNIZING THE MIDCOAST AREA VETERANS MEMORIAL WALL

● Ms. SNOWE. Mr. President, today I wish to honor and recognize with the highest esteem the many volunteers, veterans' organizations and civic and municipal entities responsible for establishing the Midcoast Area Veterans Memorial Wall in Rockland, Maine, that honors the extraordinary service and sacrifice of all our Nation's military veterans.

Established and managed by the Midcoast Area Veterans Memorial Corporation, a nonprofit corporation comprised of members from the American Legion, the Veterans of Foreign Wars (VFW), the Marine Corps League, Rockland Rotary, Rockland Kiwanis, the Benevolent and Protective Order (BPO) of Elks, and the City of Rockland, the Memorial Wall is located on upper Limerock Street in Rockland on property owned by the American Legion Post No. 1. The location of the Memorial is, appropriately, also the site of an 1861 Civil War encampment of the local Fourth Regiment of Maine Volunteers.

Undeniably, nothing unites us more as Mainers and Americans than the limitless pride we take in our revered and noble veterans. Indeed, in Maine, we also cherish the tremendous distinction of having, on any given day, the second most veterans per capita of any State in the Nation. Such devotion to country is the embodiment of the self-sacrificing principles that Mainers live by and have passed down from one generation to the next. This selfless way of thinking also inspired and motivated a small group of individuals more than 16 years ago to begin formulating plans to establish a memorial to honor our veterans in Midcoast Maine. After a long, dedicated effort and several site location changes, the Midcoast Area Veterans Memorial Wall has finally secured a permanent home.

The Midcoast Area Veterans Memorial Wall is by all accounts a beautifully designed and landscaped tribute

to the unfathomable service and sacrifice of the many Americans exceptional enough to wear the uniform—not only the 21.8 million veterans alive today, including more than 134,000 from the State of Maine, but also those who are no longer with us. Featuring stunning black granite tiles etched with digitized pictures of veterans, the wall serves as a fitting and moving tribute to those who so ably and courageously served under the Stars and Stripes to protect and preserve the cherished principles that have made our nation the greatest on earth. And, while new tiles are added twice yearly—at Memorial Day and Veterans Day—the Midcoast Area Veterans Memorial Wall is always open and provides an opportunity for each of us to express our boundless gratitude to those who have placed service above self not just on national holidays, but on every day of every month of every year.

On August 3, 2012, the Midcoast Area Veterans Memorial Wall will officially be dedicated and will feature remarks from Maine's esteemed First Lady Ann LePage, as well as officers and representatives of USCGC *Abbie Burgess*, USCGC *Tackle*, USCGC *Thunder Bay*, USS *San Antonio*, the United States Marine Corps, and the Maine Army National Guard.

On the occasion of the official dedication of the Midcoast Area Veterans Memorial Wall, I convey my deep and abiding appreciation to the many dedicated volunteers who have worked tirelessly over the past 16 years to bring this day to fruition. This faithful and successful effort exemplifies the very best of what it means to be a Mainer and an American.●

TRIBUTE TO ALLYSON BURNS

● Mr. THUNE. Mr. President, today I recognize Allyson Burns, an intern in my Rapid City, SD, office, for all of the hard work she has done for me, my staff, and the State of South Dakota over the past couple of months.

Allyson is a graduate of Stevens High School in Rapid City, SD. Currently, she is attending Creighton University in Omaha, NE where she is majoring in psychology and creative writing. She is a hard worker who has been dedicated to getting the most out of her internship experience.

I extend my sincere thanks and appreciation to Allyson for all of the fine work she has done and wish her continued success in the years to come.●

TRIBUTE TO TYLER FITZ

● Mr. THUNE. Mr. President, today I recognize Tyler Fitz, an intern in my Washington, DC, office, for all of the hard work he has done for me, my staff, and the State of South Dakota over the past several weeks.

Tyler is a graduate of Roosevelt High School in Sioux Falls, SD. He is also a graduate of South Dakota State University where he majored in history and Spanish. He is a hard worker who has been dedicated to getting the most out of his internship experience.

I extend my sincere thanks and appreciation to Tyler for all of the fine work he has done and wish him continued success in the years to come.●

TRIBUTE TO STEPHEN GOODFELLOW

● Mr. THUNE. Mr. President, today I wish to recognize Stephen Goodfellow, an intern in my Sioux Falls, SD, office, for all of the hard work he has done for me, my staff, and the State of South Dakota over the past several weeks.

Stephen is a graduate of Boiling Springs High School in Boiling Springs, PA. Currently, he is attending the University of South Dakota where he is majoring in economics and finance. He is a hard worker who has been dedicated to getting the most out of his internship experience.

I would like to extend my sincere thanks and appreciation to Stephen for all of the fine work he has done and wish him continued success in the years to come.●

TRIBUTE TO ALEX HALL

● Mr. THUNE. Mr. President, today I recognize Alex Hall, an intern in my Washington, DC, office, for all of the hard work he has done for me, my staff, and the State of South Dakota over the past several weeks.

Alex is a graduate of Lincoln High School in Sioux Falls, SD. Currently, he is attending the University of New Mexico where he is majoring in philosophy and psychology. He is a hard worker who has been dedicated to getting the most out of his internship experience.

I extend my sincere thanks and appreciation to Alex for all of the fine work he has done and wish him continued success in the years to come.●

TRIBUTE TO KODY KYRISS

● Mr. THUNE. Mr. President, today I wish to recognize Kody Kyriss, an intern in my Aberdeen, SD, office, for all of the hard work he has done for me, my staff, and the State of South Dakota over the past several weeks.

Kody is a native of Lesterville and a graduate of Menno High School. Currently, he is attending Northern State University, where he is pursuing degrees in English and political science. He is a very hard worker who has been dedicated to getting the most out of his internship experience.

I would like to extend my sincere thanks and appreciation to Kody for all of the fine work he has done and wish him continued success in the years to come.●

TRIBUTE TO MEGAN RAPOSA

● Mr. THUNE. Mr. President, today I wish to recognize Megan Raposa, an intern in my Sioux Falls, SD, office, for all of the hard work she has done for me, my staff, and the State of South Dakota over the past several weeks.

Megan is a graduate of St. Thomas More High School in Rapid City, SD. Currently, she is attending Augustana College where she is majoring in business communications and government. She is a hard worker who has been dedicated to getting the most out of her internship experience.

I would like to extend my sincere thanks and appreciation to Megan for all of the fine work she has done and wish her continued success in the years to come.●

TRIBUTE TO BRENDAN SMITH

● Mr. THUNE. Mr. President, today I recognize Brendan Smith, an intern in my Washington, DC, office, for all of the hard work he has done for me, my staff, and the State of South Dakota over the past several weeks.

Brendan is a graduate of Lyman High School in Presho, SD. Currently, he is attending South Dakota School of Mines and Technology where he is majoring in chemical engineering. He is a hard worker who has been dedicated to getting the most out of his internship experience.

I extend my sincere thanks and appreciation to Brendan for all of the fine work he has done and wish him continued success in the years to come.●

TRIBUTE TO JAMES WHITCHER

● Mr. THUNE. Mr. President, today I recognize James Whitcher, an intern in my Washington, DC, office, for all of the hard work he has done for me, my staff, and the State of South Dakota over the past several weeks.

James is a graduate of Hot Springs High School in Hot Springs, SD. Currently, he is attending the University of Mary in Bismarck, ND, where he is majoring in athletic training. He is a hard worker who has been dedicated to getting the most out of his internship experience.

I extend my sincere thanks and appreciation to James for all of the fine work he has done and wish him continued success in the years to come.●

MESSAGES FROM THE PRESIDENT

Messages from the President of the United States were communicated to the Senate by Mr. Pate, one of his secretaries.

EXECUTIVE MESSAGES REFERRED

As in executive session the Presiding Officer laid before the Senate messages from the President of the United States submitting sundry nominations which were referred to the Committee on Health, Education, Labor, and Pensions.

(The messages received today are printed at the end of the Senate proceedings.)

REPORT RELATIVE TO THE ISSUANCE OF AN EXECUTIVE ORDER TO TAKE ADDITIONAL STEPS WITH RESPECT TO THE NATIONAL EMERGENCY ORIGINALLY DECLARED ON MARCH 15, 1995 IN EXECUTIVE ORDER 12957 WITH RESPECT TO IRAN—PM 60

The PRESIDING OFFICER laid before the Senate the following message from the President of the United States, together with an accompanying report; which was referred to the Committee on Banking, Housing, and Urban Affairs:

To the Congress of the United States:

Pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (IEEPA), I hereby report that I have issued an Executive Order (the ''order'') that takes additional steps with respect to the national emergency declared in Executive Order 12957 of March 15, 1995.

In Executive Order 12957, the President found that the actions and policies of the Government of Iran threaten the national security, foreign policy, and economy of the United States. To deal with that threat, the President in Executive Order 12957 declared a national emergency and imposed prohibitions on certain transactions with respect to the development of Iranian petroleum resources. To further respond to that threat, Executive Order 12959 of May 6, 1995, imposed comprehensive trade and financial sanctions on Iran. Executive Order 13059 of August 19, 1997, consolidated and clarified the previous orders. To take additional steps with respect to the national emergency declared in Executive Order 12957 and to implement section 105(a) of the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (Public Law 111–195) (22 U.S.C. 8501 *et seq.*) (CISADA), I issued Executive Order 553 on September 28, 2010, to impose sanctions on officials of the Government of Iran and other persons acting on behalf of the Government of Iran determined to be responsible for or complicit in certain serious human rights abuses. To take further additional steps with respect to the threat posed by Iran and to provide implementing authority for a number of the sanctions set forth in the Iran Sanctions Act of 1996 (Public Law 104–172) (50 U.S.C. 1701 note) (ISA), as amended by CISADA, I issued Executive Order 13574 on May 23, 2011, to authorize the Secretary of the Treasury to implement certain sanctions imposed by the Secretary of State pursuant to ISA, as amended by CISADA. I also issued Executive Order 13590 on November 20, 2011, to take additional steps with respect to this emergency by authorizing the Secretary of State to impose sanctions on persons providing certain goods, services, technology, or support that contribute either to Iran's development of petroleum resources or to Iran's production of petrochemicals, and to authorize the Secretary of the Treasury to implement some of those sanctions. On February 5, 2012, in order to take further additional steps pursuant to this emergency, and to implement section 1245(c) of the National Defense Authorization Act for Fiscal Year 2012 (Public Law 112–81), I issued Executive Order 13599 blocking the property of the Government of Iran, all Iranian financial institutions, and persons determined to be owned or controlled by, or acting for or on behalf of, such parties. Most recently, on April 22, 2012, and May 1, 2012, I issued Executive Orders 13606 and 13608, respectively. Executive Orders 13606 and 13608 each take additional steps with respect to various emergencies, including the emergency declared in Executive Order 12957 concerning Iran, to address the use of computer and information technology to commit serious human rights abuses and efforts by foreign persons to evade sanctions.

The order takes additional steps with respect to the national emergency declared in Executive Order 12957, particularly in light of the Government of Iran's use of revenues from petroleum, petroleum products, and petrochemicals for illicit purposes; Iran's continued attempts to evade international sanctions through deceptive practices; and the unacceptable risk posed to the international financial system by Iran's activities. Subject to certain exceptions and conditions, the order authorizes the Secretary of the Treasury and the Secretary of State, as set forth in the order, to impose sanctions on persons as described in the order, all as more fully described below.

Section 1 of the order authorizes the Secretary of the Treasury, in consultation with the Secretary of State, to impose financial sanctions on foreign financial institutions determined to have knowingly conducted or facilitated certain significant financial transactions with the National Iranian Oil Company (NIOC) or Naftiran Intertrade Company (NICO), or for the purchase or acquisition of petroleum, petroleum products, or petrochemical products from Iran.

Section 2 of the order authorizes the Secretary of State, in consultation with the Secretary of the Treasury, the Secretary of Commerce, and the United States Trade Representative, and with the President of the Export-Import Bank, the Chairman of the Board of Governors of the Federal Reserve System, and other agencies and officials as appropriate, to impose any of a number of sanctions on a person upon determining that the person: knowingly engaged in a significant transaction for the purchase or acquisition of petroleum, petroleum products, or petrochemical products from Iran; is a successor entity to a person determined to meet the criterion above; owns or controls a person determined to meet the criterion above, and had knowledge that the person engaged in the activities referred to therein; or is owned or controlled by, or under common ownership or control with, a person determined to meet the criterion above, and knowingly participated in the activities referred to therein.

Sections 3 and 4 of the order provide that, for persons determined to meet any of the criteria specified in section 2 of the order, the heads of the relevant agencies, in consultation with the Secretary of State, shall implement the sanctions imposed by the Secretary of State. The sanctions provided for in sections 3 and 4 of the order include the following actions: the Board of Directors of the Export-Import Bank shall deny approval of the issuance of any guarantee, insurance, extension of credit, or participation in an extension of credit in connection with the export of any goods or services to the sanctioned person; agencies shall not issue any specific license or grant any other specific permission or authority under any statute that requires the prior review and approval of the United States Government as a condition for the export or reexport of goods or technology to the sanctioned person; for a sanctioned person that is a financial institution: the Chairman of the Board of Governors of the Federal Reserve System and the President of the Federal Reserve Bank of New York shall take such actions as they deem appropriate, including denying designation, or terminating the continuation of any prior designation of, the sanctioned person as a primary dealer in United States Government debt instruments; or agencies shall prevent the sanctioned person from serving as an agent of the United States Government or serving as a repository for United States Government funds; agencies shall not procure, or enter into a contract for the procurement of, any goods or services from the sanctioned person; the Secretary of the Treasury shall take actions where necessary to: prohibit any United States financial institution from making loans or providing credits to the sanctioned person totaling more than $10,000,000 in any 12-month period unless such person is engaged in activities to relieve human suffering and the loans or credits are provided for such activities; prohibit any transactions in foreign exchange that are subject to the jurisdiction of the United States and in which the sanctioned person has any interest; prohibit any transfers of credit or payments between financial institutions or by, through, or to any financial institution, to the extent that such transfers or payments are subject to the jurisdiction of the United States and involve any interest of the sanctioned person; block all property and interests in property that are in the United States, that come within the United States, or that are or come within the possession or control of any United States person, including any foreign branch, of the sanctioned person, and provide that such property and interests in property may not be transferred, paid, exported, withdrawn, or otherwise dealt in; or restrict or

prohibit imports of goods, technology, or services, directly or indirectly, into the United States from the sanctioned person.

Section 5 of the order authorizes the Secretary of the Treasury, in consultation with the Secretary of State, to block all property and interests in property that are in the United States, that come within the United States, or that are or come within the possession or control of any United States person, including any foreign branch, of any person upon determining that the person has materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, NIOC, NICO, or the Central Bank of Iran, or the purchase or acquisition of U.S. bank notes or precious metals by the Government of Iran.

I have delegated to the Secretary of the Treasury the authority, in consultation with the Secretary of State, to take such actions, including the promulgation of rules and regulations, and to employ all powers granted to the President by IEEPA, as may be necessary to carry out the purposes of sections 1, 4, and 5 of the order.

The order was effective at 12:01 a.m. eastern daylight time on July 31, 2012. All agencies of the United States Government are directed to take all appropriate measures within their authority to carry out the provisions of the order.

I am enclosing a copy of the Executive Order I have issued.

BARACK OBAMA.

THE WHITE HOUSE, *July 30, 2012*.

MEASURES PLACED ON THE CALENDAR

The following bills were read the second time, and placed on the calendar:

S. 3457. A bill to require the Secretary of Veterans Affairs to establish a veterans jobs corps, and for other purposes.

H.R. 4078. An act to provide that no agency may take any significant regulatory action until the unemployment rate is equal to or less than 6.0 percent.

REPORTS OF COMMITTEES

The following reports of committees were submitted:

By Mr. LIEBERMAN, from the Committee on Homeland Security and Governmental Affairs:

Special Report entitled ''Activities of the Committee on Homeland Security and Governmental Affairs During the 111th Congress'' (Rept. No. 112-193).

By Mr. KERRY, from the Committee on Foreign Relations, without amendment:

S. 641. A bill to provide 100,000,000 people with first-time access to safe drinking water and sanitation on a sustainable basis within six years by improving the capacity of the United States Government to fully implement the Senator Paul Simon Water for the Poor Act of 2005 (Rept. No. 112-09194).

By Mr. AKAKA, from the Committee on Indian Affairs, without amendment:

H.R. 1560. A bill to amend the Ysleta del Sur Pueblo and Alabama and Coushatta Indian Tribes of Texas Restoration Act to allow the Ysleta del Sur Pueblo Tribe to determine blood quantum requirement for membership in that tribe.

By Mr. LIEBERMAN, from the Committee on Homeland Security and Governmental Affairs, with an amendment in the nature of a substitute:

S. 792. A bill to authorize the waiver of certain debts relating to assistance provided to individuals and households since 2005.

By Mr. ROCKEFELLER, from the Committee on Commerce, Science, and Transportation, without amendment:

S. 3410. A bill to extend the Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006, and for other purposes.

EXECUTIVE REPORTS OF COMMITTEE

The following executive reports of nominations were submitted:

By Mr. ROCKEFELLER for the Committee on Commerce, Science, and Transportation.

*National Oceanic and Atmospheric Administration nomination of Gerd F. Glang, to be Rear Admiral (lower half).

*National Oceanic and Atmospheric Administration nomination of Michael S. Devany, to be Rear Admiral.

*National Oceanic and Atmospheric Administration nomination of David A. Score, to be Rear Admiral (lower half).

*William P. Doyle, of Pennsylvania, to be a Federal Maritime Commissioner for the term expiring June 30, 2013.

*Michael Peter Huerta, of the District of Columbia, to be Administrator of the Federal Aviation Administration for the term of five years.

*Patricia K. Falcone, of California, to be an Associate Director of the Office of Science and Technology Policy.

*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.

EXECUTIVE REPORT OF COMMITTEE—TREATY

The following executive report of committee was submitted:

By Mr. KERRY, from the Committee on Foreign Relations:

Treaty Doc. 112–7 Convention on the Rights of Persons with Disabilities with 3 reservations, 8 understandings, and 2 declarations (Ex. Rept. 112–6)

TEXT OF THE COMMITTEE-RECOMMENDED RESOLUTION OF ADVICE AND CONSENT TO RATIFICATION

Resolved, (two-thirds of the Senators present concurring therein),

That the Senate advises and consents to the ratification of the Convention on the Rights of Persons with Disabilities, adopted by the United Nations General Assembly on December 13, 2006, and signed by the United States of America on June 30, 2009 (''the Convention'') (Treaty Doc. 112–7), subject to the reservations of subsection (a), the understandings of subsection (b), and the declarations of subsection (c).

(a) Reservations.—The advice and consent of the Senate to the ratification of the Convention is subject to the following reservations, which shall be included in the instrument of ratification:

(1) This Convention shall be implemented by the Federal Government of the United States of America to the extent that it exercises legislative and judicial jurisdiction over the matters covered therein, and otherwise by the state and local governments; to the extent that state and local governments exercise jurisdiction over such matters, the obligations of the United States of America under the Convention are limited to the Federal Government's taking measures appropriate to the Federal system, which may include enforcement action against state and local actions that are inconsistent with the Constitution, the Americans with Disabilities Act, or other Federal laws, with the ultimate objective of fully implementing the Convention.

(2) The Constitution and laws of the United States of America establish extensive protections against discrimination, reaching all forms of governmental activity as well as significant areas of non-governmental activity. Individual privacy and freedom from governmental interference in certain private conduct are also recognized as among the fundamental values of our free and democratic society. The United States of America understands that by its terms the Convention can be read to require broad regulation of private conduct. To the extent it does, the United States of America does not accept any obligation under the Convention to enact legislation or take other measures with respect to private conduct except as mandated by the Constitution and laws of the United States of America.

(3) Article 15 of the Convention memorializes existing prohibitions on torture and other cruel, inhuman, or degrading treatment or punishment contained in Articles 2 and 16 of the United Nations Convention Against Torture and other Cruel, Inhuman, or Degrading Treatment or Punishment (CAT) and in Article 7 of the International Covenant on Civil and Political Rights (ICCPR), and further provides that such protections shall be extended on an equal basis with respect to persons with disabilities. To ensure consistency of application, the obligations of the United States of America under Article 15 shall be subject to the same reservations and understandings that apply for the United States of America with respect to Articles 1 and 16 of the CAT and Article 7 of the ICCPR.

(b) Understandings.—The advice and consent of the Senate to the ratification of the Convention is subject to the following understandings, which shall be included in the instrument of ratification:

(1) The United States of America understands that this Convention, including Article 8 thereof, does not authorize or require legislation or other action that would restrict the right of free speech, expression, and association protected by the Constitution and laws of the United States of America.

(2) Given that under Article 1 of the Convention ''[t]he purpose of the present Convention is to promote, protect, and ensure the full and equal enjoyment of all human rights and fundamental freedoms by all persons with disabilities,'' with respect to the application of the Convention to matters related to economic, social, and cultural rights, including in Articles 4(2), 24, 25, 27, 28 and 30, the United States of America understands that its obligations in this respect are to prevent discrimination on the basis of disability in the provision of any such rights insofar as they are recognized and implemented under U.S. Federal law.

(3) Current U.S. law provides strong protections for persons with disabilities against unequal pay, including the right to equal pay for equal work. The United States of America understands the Convention to require

the protection of rights of individuals with disabilities on an equal basis with others, including individuals in other protected groups, and does not require adoption of a comparable worth framework for persons with disabilities.

(4) Article 27 of the Convention provides that States Parties shall take appropriate steps to afford to individuals with disabilities the right to equal access to equal work, including nondiscrimination in hiring and promotion of employment of persons with disabilities in the public sector. Current interpretation of Section 501 of the Rehabilitation Act of 1973 exempts U.S. Military Departments charged with defense of the national security from liability with regard to members of the uniformed services. The United States of America understands the obligations of Article 27 to take appropriate steps as not affecting hiring, promotion, or other terms or conditions of employment of uniformed employees in the U.S. Military Departments, and that Article 27 does not recognize rights in this regard that exceed those rights available under U.S. Federal law.

(5) The United States of America understands that the terms ''disability,'' ''persons with disabilities,'' and ''undue burden'' (terms that are not defined in the Convention), ''discrimination on the basis of disability,'' and ''reasonable accommodation'' are defined for the United States of America coextensively with the definitions of such terms pursuant to relevant United States law.

(6) The United States of America understands that the Committee on the Rights of Persons with Disabilities, established under Article 34 of the Convention, is authorized under Article 36 to ''consider'' State Party Reports and to ''make such suggestions and general recommendations on the report as it may consider appropriate.'' Under Article 37, the committee ''shall give due consideration to ways and means of enhancing national capacities for the implementation of the present Convention.'' The United States of America understands that the Committee on the Rights of Persons with Disabilities has no authority to compel actions by states parties, and the United States of America does not consider conclusions, recommendations, or general comments issued by the committee as constituting customary international law or to be legally binding on the United States in any manner.

(7) The United States of America understands that the Convention is a non-discrimination instrument. Therefore, nothing in the Convention, including Article 25, addresses the provision of any particular health program or procedure. Rather, the Convention requires that health programs and procedures are provided to individuals with disabilities on a non-discriminatory basis.

(8) The United States of America understands that, for the United States of America, the term or principle of the ''best interests of the child'' as used in Article 7(2), will be applied and interpreted to be coextensive with its application and interpretation under United States law. Consistent with this understanding, nothing in Article 7 requires a change to existing United States law.

c. Declarations.—The advice and consent of the Senate to the ratification of the Convention is subject to the following declarations:

The United States of America declares that the provisions of the Convention are not self-executing.

The Senate declares that, in view of the reservations to be included in the instrument of ratification, current United States law fulfills or exceeds the obligations of the Convention for the United States of America.

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. BINGAMAN (for himself, Mr. ALEXANDER, and Mr. DURBIN):

S. 3459. A bill to amend the Department of Energy High-End Computing Revitalization Act of 2004 to improve the high-end computing research and development program of the Department of Energy, and for other purposes; to the Committee on Energy and Natural Resources.

By Mr. COONS (for himself, Mr. ENZI, Mr. SCHUMER, and Mr. RUBIO):

S. 3460. A bill to amend the Internal Revenue Code of 1986 to provide for startup businesses to use a portion of the research and development credit to offset payroll taxes; to the Committee on Finance.

By Mr. BROWN of Ohio (for himself, Mr. WICKER, Mr. KERRY, Mr. BLUMENTHAL, Mr. WHITEHOUSE, and Mr. BEGICH):

S. 3461. A bill to amend title IV of the Public Health Service Act to provide for a National Pediatric Research Network, including with respect to pediatric rare diseases or conditions; to the Committee on Health, Education, Labor, and Pensions.

By Mr. LEAHY (for himself, Mr. GRASSLEY, and Mr. KOHL):

S. 3462. A bill to provide anti-retaliation protections for antitrust whistleblowers; to the Committee on the Judiciary.

By Mr. FRANKEN (for himself, Mr. LUGAR, Mr. ROCKEFELLER, Ms. COLLINS, Mrs. SHAHEEN, Mr. WYDEN, Mr. BLUMENTHAL, and Mr. BROWN of Ohio):

S. 3463. A bill to amend title XVIII of the Social Security Act to reduce the incidence of diabetes among Medicare beneficiaries; to the Committee on Finance.

By Mr. JOHNSON of South Dakota:

S. 3464. A bill to amend the Mni Wiconi Project Act of 1988 to facilitate completion of the Mni Wiconi Rural Water Supply System, and for other purposes; to the Committee on Energy and Natural Resources.

By Mr. JOHNSON of Wisconsin:

S.J. Res. 48. A joint resolution disapproving the rule submitted by the Internal Revenue Service relating to the health insurance premium tax credit; to the Committee on Finance.

SUBMISSION OF CONCURRENT AND SENATE RESOLUTIONS

The following concurrent resolutions and Senate resolutions were read, and referred (or acted upon), as indicated:

By Mr. MANCHIN:

S. Res. 534. A resolution congratulating the Navy Dental Corps on its 100th anniversary; to the Committee on Armed Services.

ADDITIONAL COSPONSORS

S. 19

At the request of Mr. HATCH, the name of the Senator from North Dakota (Mr. HOEVEN) was added as a cosponsor of S. 19, a bill to restore American's individual liberty by striking the Federal mandate to purchase insurance.

S. 202

At the request of Mr. PAUL, the name of the Senator from Illinois (Mr. KIRK) was added as a cosponsor of S. 202, a bill to require a full audit of the Board of Governors of the Federal Reserve System and the Federal reserve banks by the Comptroller General of the United States before the end of 2012, and for other purposes.

S. 225

At the request of Ms. KLOBUCHAR, the names of the Senator from California (Mrs. FEINSTEIN), the Senator from New York (Mr. SCHUMER) and the Senator from Rhode Island (Mr. WHITEHOUSE) were added as cosponsors of S. 225, a bill to permit the disclosure of certain information for the purpose of missing child investigations.

S. 339

At the request of Mr. BAUCUS, the name of the Senator from North Carolina (Mrs. HAGAN) was added as a cosponsor of S. 339, a bill to amend the Internal Revenue Code of 1986 to make permanent the special rule for contributions of qualified conservation contributions.

S. 362

At the request of Mr. WHITEHOUSE, the name of the Senator from New Hampshire (Mrs. SHAHEEN) was added as a cosponsor of S. 362, a bill to amend the Public Health Service Act to provide for a Pancreatic Cancer Initiative, and for other purposes.

S. 678

At the request of Mr. KOHL, the name of the Senator from Iowa (Mr. GRASSLEY) was added as a cosponsor of S. 678, a bill to increase the penalties for economic espionage.

S. 818

At the request of Mr. KERRY, the name of the Senator from Rhode Island (Mr. WHITEHOUSE) was added as a cosponsor of S. 818, a bill to amend title XVIII of the Social Security Act to count a period of receipt of outpatient observation services in a hospital toward satisfying the 3-day inpatient hospital requirement for coverage of skilled nursing facility services under Medicare.

S. 845

At the request of Mr. ENZI, the name of the Senator from Alaska (Mr. BEGICH) was added as a cosponsor of S. 845, a bill to amend the Internal Revenue Code of 1986 to provide for the logical flow of return information between partnerships, corporations, trusts, estates, and individuals to better enable each party to submit timely, accurate returns and reduce the need for extended and amended returns, to provide for modified due dates by regulation, and to conform the automatic corporate extension period to longstanding regulatory rule.

S. 847

At the request of Mr. LAUTENBERG, the name of the Senator from Hawaii (Mr. AKAKA) was added as a cosponsor of S. 847, a bill to amend the Toxic Substances Control Act to ensure that risks from chemicals are adequately understood and managed, and for other purposes.

S. 1269

At the request of Ms. SNOWE, the names of the Senator from Maryland (Mr. CARDIN) and the Senator from Rhode Island (Mr. REED) were added as cosponsors of S. 1269, a bill to amend the Elementary and Secondary Education Act of 1965 to require the Secretary of Education to collect information from coeducational secondary schools on such schools' athletic programs, and for other purposes.

S. 1366

At the request of Ms. CANTWELL, the name of the Senator from Minnesota (Mr. FRANKEN) was added as a cosponsor of S. 1366, a bill to amend the Internal Revenue Code of 1986 to broaden the special rules for certain governmental plans under section 105(j) to include plans established by political subdivisions.

S. 1878

At the request of Mr. MENENDEZ, the name of the Senator from Maine (Ms. COLLINS) was added as a cosponsor of S. 1878, a bill to assist low-income individuals in obtaining recommended dental care.

S. 1935

At the request of Ms. COLLINS, the name of the Senator from North Dakota (Mr. HOEVEN) was added as a cosponsor of S. 1935, a bill to require the Secretary of the Treasury to mint coins in recognition and celebration of the 75th anniversary of the establishment of the March of Dimes Foundation.

S. 1990

At the request of Mr. LIEBERMAN, the name of the Senator from Georgia (Mr. ISAKSON) was added as a cosponsor of S. 1990, a bill to require the Transportation Security Administration to comply with the Uniformed Services Employment and Reemployment Rights Act.

S. 2074

At the request of Mr. CARDIN, the name of the Senator from Michigan (Ms. STABENOW) was added as a cosponsor of S. 2074, a bill to amend the Internal Revenue Code of 1986 to expand the rehabilitation credit, and for other purposes.

S. 2078

At the request of Mr. MENENDEZ, the name of the Senator from Nevada (Mr. HELLER) was added as a cosponsor of S. 2078, a bill to enable Federal and State chartered banks and thrifts to meet the credit needs of the Nation's home builders, and to provide liquidity and ensure stable credit for meeting the Nation's need for new homes.

S. 2148

At the request of Mr. INHOFE, the name of the Senator from Alabama (Mr. SESSIONS) was added as a cosponsor of S. 2148, a bill to amend the Toxic Substance Control Act relating to lead-based paint renovation and remodeling activities.

S. 2189

At the request of Mr. HARKIN, the name of the Senator from Alaska (Mr. BEGICH) was added as a cosponsor of S. 2189, a bill to amend the Age Discrimination in Employment Act of 1967 and other laws to clarify appropriate standards for Federal antidiscrimination and antiretaliation claims, and for other purposes.

S. 2245

At the request of Mr. BARRASSO, the name of the Senator from North Carolina (Mr. BURR) was added as a cosponsor of S. 2245, a bill to preserve existing rights and responsibilities with respect to waters of the United States.

S. 2268

At the request of Mrs. GILLIBRAND, the name of the Senator from Montana (Mr. TESTER) was added as a cosponsor of S. 2268, a bill to ensure that all items offered for sale in any gift shop of the National Park Service or of the National Archives and Records Administration are produced in the United States, and for other purposes.

S. 2320

At the request of Ms. AYOTTE, the name of the Senator from Indiana (Mr. COATS) was added as a cosponsor of S. 2320, a bill to direct the American Battle Monuments Commission to provide for the ongoing maintenance of Clark Veterans Cemetery in the Republic of the Philippines, and for other purposes.

S. 2620

At the request of Mr. SCHUMER, the names of the Senator from Wisconsin (Mr. KOHL) and the Senator from New Mexico (Mr. BINGAMAN) were added as cosponsors of S. 2620, a bill to amend title XVIII of the Social Security Act to provide for an extension of the Medicare-dependent hospital (MDH) program and the increased payments under the Medicare low-volume hospital program.

S. 3204

At the request of Mr. JOHANNS, the name of the Senator from Illinois (Mr. KIRK) was added as a cosponsor of S. 3204, a bill to address fee disclosure requirements under the Electronic Fund Transfer Act, and for other purposes.

S. 3236

At the request of Mr. PRYOR, the name of the Senator from Massachusetts (Mr. BROWN) was added as a cosponsor of S. 3236, a bill to amend title 38, United States Code, to improve the protection and enforcement of employment and reemployment rights of members of the uniformed services, and for other purposes.

S. 3405

At the request of Mr. HELLER, the name of the Senator from South Dakota (Mr. THUNE) was added as a cosponsor of S. 3405, a bill to amend title 38, United States Code, to treat small businesses bequeathed to spouses and dependents by members of the Armed Forces killed in line of duty as small business concerns owned and controlled by veterans for purposes of Department of Veterans Affairs contracting goals and preferences, and for other purposes.

S. 3430

At the request of Mrs. SHAHEEN, the name of the Senator from Minnesota (Ms. KLOBUCHAR) was added as a cosponsor of S. 3430, a bill to amend the Public Health Service Act to foster more effective implementation and coordination of clinical care for people with pre-diabetes and diabetes.

S. 3450

At the request of Mr. COATS, the name of the Senator from Alaska (Ms. MURKOWSKI) was added as a cosponsor of S. 3450, a bill to limit the authority of the Secretary of the Interior to issue regulations before December 31, 2013, under the Surface Mining Control and Reclamation Act of 1977.

S. 3458

At the request of Mr. LAUTENBERG, the names of the Senator from California (Mrs. BOXER) and the Senator from Hawaii (Mr. AKAKA) were added as cosponsors of S. 3458, a bill to require face to face purchases of ammunition, to require licensing of ammunition dealers, and to require reporting regarding bulk purchases of ammunition.

S.J. RES. 29

At the request of Mr. UDALL of New Mexico, the name of the Senator from California (Mrs. BOXER) was added as a cosponsor of S.J. Res. 29, a joint resolution proposing an amendment to the Constitution of the United States relating to contributions and expenditures intended to affect elections.

S.J. RES. 43

At the request of Mrs. FEINSTEIN, the name of the Senator from Minnesota (Ms. KLOBUCHAR) was added as a cosponsor of S.J. Res. 43, a joint resolution approving the renewal of import restrictions contained in the Burmese Freedom and Democracy Act of 2003, and for other purposes.

S. CON. RES. 50

At the request of Mr. RUBIO, the name of the Senator from Pennsylvania (Mr. TOOMEY) was added as a cosponsor of S. Con. Res. 50, a concurrent resolution expressing the sense of Congress regarding actions to preserve and advance the multistakeholder governance model under which the Internet has thrived.

S. RES. 490

At the request of Mrs. BOXER, the name of the Senator from Massachusetts (Mr. KERRY) was added as a cosponsor of S. Res. 490, a resolution designating the week of September 16, 2012, as ''Mitochondrial Disease Awareness Week'', reaffirming the importance of an enhanced and coordinated research effort on mitochondrial diseases, and commending the National Institutes of Health for its efforts to improve the understanding of mitochondrial diseases.

S. RES. 524

At the request of Mr. KERRY, the names of the Senator from Michigan (Mr. LEVIN) and the Senator from Maine (Ms. COLLINS) were added as cosponsors of S. Res. 524, a resolution reaffirming the strong support of the

United States for the 2002 declaration of conduct of parties in the South China Sea among the member states of ASEAN and the People's Republic of China, and for other purposes.

AMENDMENT NO. 2574

At the request of Mrs. HUTCHISON, the name of the Senator from Missouri (Mrs. MCCASKILL) was added as a cosponsor of amendment No. 2574 intended to be proposed to S. 3414, a bill to enhance the security and resiliency of the cyber and communications infrastructure of the United States.

AMENDMENT NO. 2617

At the request of Mr. COONS, the name of the Senator from Illinois (Mr. DURBIN) was added as a cosponsor of amendment No. 2617 intended to be proposed to S. 3414, a bill to enhance the security and resiliency of the cyber and communications infrastructure of the United States.

AMENDMENT NO. 2618

At the request of Mr. AKAKA, the names of the Senator from New Hampshire (Mrs. SHAHEEN) and the Senator from Illinois (Mr. DURBIN) were added as cosponsors of amendment No. 2618 intended to be proposed to S. 3414, a bill to enhance the security and resiliency of the cyber and communications infrastructure of the United States.

AMENDMENT NO. 2636

At the request of Ms. SNOWE, the name of the Senator from Missouri (Mrs. MCCASKILL) was added as a cosponsor of amendment No. 2636 intended to be proposed to S. 3414, a bill to enhance the security and resiliency of the cyber and communications infrastructure of the United States.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. BINGAMAN (for himself, Mr. ALEXANDER, and Mr. DURBIN):

S. 3459. A bill to amend the Department of Energy High-End Computing Revitalization Act of 2004 to improve the high-end computing research and development program of the Department of Energy, and for other purposes; to the Committee on Energy and Natural Resources.

Mr. BINGAMAN. Mr. President, I am pleased to introduce the Department of Energy High-End Computing Improvement Act of 2012, along with my cosponsors, Senators ALEXANDER and DURBIN. This bipartisan bill addresses the need for ongoing high performance computing and the establishment of an exascale program within the Department of Energy, DOE.

America's leadership in high performance computing, HPC, is essential to a vast range of national priorities in science, energy, environment, health, and national security. For decades the U.S. was the leader in HPC through collaborative efforts led by the DOE between national laboratories, academia, and industry. Investments in HPC have facilitated extraordinary scientific and technological advances that have enabled a wide range of simulation and analysis saving time, money, energy and fuel, which has strengthened the U.S. economy and contributed to national security.

U.S. leadership in HPC has recently been challenged through significant governmental investment in HPC programs in Japan, China, South Korea, Russia, and the European Union, and the race to exascale computing is on. Exascale computers will be able to perform 10 to the 18th power floating point operations per second making them 1000 times more powerful than the most advanced computers today. These new computers will require the development of new software and computer architectures with improved power consumption, memory, and reliability.

This bipartisan bill updates the Department of Energy High-End Computing Revitalization Act of 2004 to preserve DOE HPC and to distinguish the exascale initiative from other high-end computing efforts. Based on input from the DOE, appropriate funding levels are established through this bill to support the exascale initiative through fiscal year 2015. This bill will ensure that the U.S. remains competitive in the race to exascale and as with previous generations of HPC systems, the resulting technological advances will further support Federal priorities like research and national security and will be integrated into electronics industries strengthening high-tech competitiveness and driving economic growth.

I would like to conclude by taking a moment to acknowledge the exceptional efforts of a few staff members who have worked diligently to help craft this important piece of legislation. Jonathan Epstein, a former staff member on my Energy and Natural Resources Committee and current staff member on the Armed Services Committee and Jennifer Nekuda Malik, a AAAS Science Policy Fellow on my Energy and Natural Resources Committee worked with Neena Imam, a Legislative Fellow on Senator ALEXANDER's staff and Tom Craig, a staff member on the Appropriations Committee, to update the DOE's high-end computing program to account for changes since the Department of Energy High-End Computing Revitalization Act of 2004 and establish the exascale computing program. I appreciate the efforts of these staff members and I thank them for their work.

Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

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

S. 3459

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 ''Department of Energy High-End Computing Improvement Act of 2012''.

SEC. 2. RENAMING OF ACT.

(a) IN GENERAL.—Section 1 of the Department of Energy High-End Computing Revitalization Act of 2004 (15 U.S.C. 5501 note; Public Law 108–423) is amended by striking ''Department of Energy High-End Computing Revitalization Act of 2004'' and inserting ''Department of Energy High-End Computing Act of 2012''.

(b) CONFORMING AMENDMENT.—Section 976(a)(1) of the Energy Policy Act of 2005 (42 U.S.C. 16316(1)) is amended by striking ''Department of Energy High-End Computing Revitalization Act of 2004'' and inserting ''Department of Energy High-End Computing Act of 2012''.

SEC. 3. DEFINITIONS.

Section 2 of the Department of Energy High-End Computing Act of 2012 (15 U.S.C. 5541) is amended—

(1) by redesignating paragraphs (2) through (5) as paragraphs (3) through (6), respectively;

(2) by striking paragraph (1) and inserting the following:

''(1) DEPARTMENT.—The term 'Department' means the Department of Energy.

''(2) EXASCALE COMPUTING.—The term 'exascale computing' means computing through the use of a computing machine that performs near or above 10 to the 18th power floating point operations per second.''; and

(3) in paragraph (6) (as redesignated by paragraph (1)), by striking '', acting through the Director of the Office of Science of the Department of Energy''.

SEC. 4. DEPARTMENT OF ENERGY HIGH-END COMPUTING RESEARCH AND DEVELOPMENT PROGRAM.

Section 3 of the Department of Energy High-End Computing Act of 2012 (15 U.S.C. 5542) is amended—

(1) in subsection (a)(1), by striking ''program'' and inserting ''coordinated program across the Department'';

(2) in subsection (b)(2), by striking '', which may'' and all that follows through ''architectures''; and

(3) by striking subsection (d) and inserting the following:

''(d) EXASCALE COMPUTING PROGRAM.—

''(1) IN GENERAL.—The Secretary shall conduct a research program (referred to in this subsection as the 'program') to develop 1 or more exascale computing machines to promote the missions of the Department.

''(2) COORDINATION.—In carrying out the program, the Secretary shall coordinate the development of 1 or more exascale computing machines across all applicable agencies of the Department.

''(3) CODESIGN.—The Secretary shall carry out the program through an integration of application, computer science, and computer hardware architecture using public-private partnerships to ensure that, to the maximum extent practicable, 1 or more exascale computing machines are capable of solving Department target applications and scientific problems.

''(4) MERIT REVIEW.—The development of 1 or more exascale computing machines shall be conducted through a merit review process.

''(5) ANNUAL REPORTS.—At the time of the budget submission of the Department for each fiscal year, the Secretary shall submit to Congress a report that describes funding for the exascale computing program as a whole by functional element of the Department and critical milestones.''.

SEC. 5. AUTHORIZATION OF APPROPRIATIONS.

Section 4 of the Department of Energy High-End Computing Act of 2012 (15 U.S.C. 5543) is amended—

(1) by striking ''this Act'' and inserting ''section 3(d)''; and

(2) by striking paragraphs (1) through (3) and inserting the following:

''(1) $110,000,000 for fiscal year 2013;

''(2) $220,000,000 for fiscal year 2014; and

''(3) $300,000,000 for fiscal year 2015.''.

By Mr. COONS (for himself, Mr. ENZI, Mr. SCHUMER, and Mr. RUBIO):

S. 3460. A bill to amend the Internal Revenue Code of 1986 to provide for startup businesses to use a portion of the research and development credit to offset payroll taxes; to the Committee on Finance.

Mr. COONS. Mr. President, to fuel American economic growth and job creation, we have to make sure our tax policy is as smart as the innovators who power our economy.

American ingenuity has always been at the core of our economic success. Behind nearly every game-changing innovation, from the light bulb to the search engine, has been critical research and development that transforms an idea into a market-ready product. The challenges of the global economy may be new, but the solution is the same—supporting and sustaining American innovators.

That is why I joined with my friend and colleague, the Senator from Wyoming, Senator ENZI, to draft legislation that gives innovative startup companies the opportunity to take advantage of the successful research and development tax credit, which would support their efforts to invest in innovation and create jobs.

Senator ENZI and I are proud to be joined by Senator SCHUMER of New York and Senator RUBIO of Florida in introducing the Startup Innovation Credit Act of 2012, which allows qualifying companies to claim the R&D tax credit against their employment taxes instead of their income taxes, thereby opening the credit to new companies who don't yet have an income tax liability. We are also grateful to our colleagues in the House, who are working to introduce a bipartisan companion bill this week.

Over the past three decades, the research and development tax credit has helped tens of thousands of successful American companies create jobs by incentivizing investment in innovation. But with America's global manufacturing competitiveness at stake, it is time Congress shows the same type of support for entrepreneurs and young companies.

Small and startup businesses are driving our Nation's economic recovery and creating jobs by taking risks to turn their ideas into marketable products. Over the past few decades, firms that were younger than 5 years old were responsible for the overwhelming majority of new jobs in this country.

The tax code is a powerful tool in the government's toolbox, but tax credits can't help emerging companies that don't yet have tax liabilities. That takes the R&D tax credit off the table for countless promising startups and small businesses.

Over the last two years, I have talked with dozens of business leaders and experts in tax policy to refine an idea to create a new small business innovation credit that would help those young companies. My commitment to this concept has only strengthened since I introduced a version of it in my very first bill as a Senator, the Job Creation Through Innovation Act. This work continued, along with Senator RUBIO, in the subsequent AGREE Act and Startup Act 2.0.

The reason I am so doggedly pursuing this idea is because it is critical for young, innovative companies in my home state of Delaware. Take, for example, DeNovix, a small company based in Wilmington. With just six employees, they design, manufacture and sell laboratory equipment that helps scientists innovate and achieve results. As a brand-new company, all of DeNovix' products are in the research and development phase. So at this point, they can't take advantage of the R&D tax credit. A new, innovative company, shut out of support they need at the time they need it most. That seems counterproductive for our economy. So let us fix it. Under the Startup Innovation Credit Act of 2012, DeNovix and companies like them across Delaware and across the country could grow and create jobs with the help of the R&D tax credit.

We can't let tough economic times slow down the power of American ingenuity, especially when history has taught us that now is exactly the time we need to be investing in our innovators. More than half of our Fortune 500 companies were launched during a recession or bear market, so a small business founded this year could become the next General Electric or DuPont if it gets the support it needs.

America's researchers, business leaders, innovators and entrepreneurs are already working to help create jobs and ensure American competitiveness in the global economy. We just have to support and sustain their hard work, and we cannot take the rest of the year off just because there is an election coming up. Even in this difficult, partisan atmosphere, we have to find ways to work together and get things done.

Innovation will drive American economic competitiveness for generations to come, and our job is to help our innovators and entrepreneurs do their jobs. I urge my colleagues to join Senators ENZI, SCHUMER, RUBIO and I in strong support of the Startup Innovation Credit Act of 2012.

By Mr. BROWN of Ohio (for himself, Mr. WICKER, Mr. KERRY, Mr. BLUMENTHAL, Mr. WHITEHOUSE, and Mr. BEGICH):

S. 3461. A bill to amend title IV of the Public Health Service Act to provide for a National Pediatric Research Network, including with respect to pediatric rare diseases or conditions; to the Committee on Health, Education, Labor, and Pensions.

Mr. BROWN of Ohio. Mr. President, over the last few years, our country has grappled with rising health care costs.

While we are making strides, there is one area of health care that is lagging behind: pediatric research.

Children comprise 20 percept of the U.S. population, but only about 5 percent of the National Institutes of Health, NIH, extramural research is dedicated to pediatric research.

If this rate of investment is not expanded, discoveries of new treatments and therapies for some of the most devastating childhood diseases and conditions will be hindered, and the next generation of researchers will be discouraged from entering into the field of pediatrics.

That is why I have introduced the National Pediatric Research Network Act. This act seeks to reverse this trend by strengthening and expanding NIH's investments into pediatric research.

This expanded investment will help accelerate new discoveries and directly affect the health and well-being of children throughout our Nation.

My home State of Ohio is home to world-class researchers at topnotch research hospitals and universities.

We must give these institutions, including Cincinnati Children's, Rainbow Babies, Children's Hospital, and Nationwide Children's Hospitals, the resources to partner with other leading researchers across the country.

This legislation creates such an opportunity.

The centerpiece of the legislation will be the authorization of up to 20 National Pediatric Research Consortia.

They are modeled after the exemplary National Cancer Institute, NCI, Centers to help finance efficient and effective, inter-institutional pediatric research.

While NIH is working to advance translational research through Clinical & Translational Science Awards, those centers are far-reaching and focused primarily on adult diseases and clinical research. In contrast, these pediatric centers would be solely dedicated toward pediatric research.

Unlike existing NIH initiatives in which only the largest research institutions receive funds, the legislation envisions that each center will operate in a ''hub and spoke'' framework with one central academic center coordinating research and/or clinical work at numerous auxiliary sites. Encouraging collaboration can help ensure efficiency.

Furthermore, this legislation will encourage research in pediatric rare diseases.

While each rare disease or disorder affects a small patient population, it is important to note that 7,000 rare diseases—such as epidermolysis bullosa, sickle cell anemia, spinal muscular atrophy, Down syndrome, Duchene's muscular dystrophy, and many childhood cancers—affect a combined 30 million Americans and their families.

What is even more devastating is the fact that children with rare genetic diseases account for more than half of the rare disease population in the United States.

As anyone with a rare disease or disorder knows, these patient populations face unique challenges.

It is my hope the National Pediatric Research Network Act will increase our understanding of pediatric diseases, improve treatment and therapies, and create better health care outcomes for our nation's children.

I thank Senators WICKER, WHITEHOUSE, KERRY, BLUMENTHAL, and BEGICH for joining me as original cosponsors.

By Mr. LEAHY (for himself, Mr. GRASSLEY, and Mr. KOHL):

S. 3462. A bill to provide anti-retaliation protections for antitrust whistleblowers; to the Committee on the Judiciary.

Mr. LEAHY. Mr. President, I am pleased to join with Senator GRASSLEY and today introduce the Criminal Antitrust Anti-Retaliation Act. This legislation will provide important protections to employees who come forward and disclose to law enforcement price fixing and other criminal antitrust behavior that harm consumers. Senator GRASSLEY and I have a long history of working together on whistleblower issues, and I am glad we can continue this partnership today.

Whistleblowers are instrumental in alerting the public, Congress, and law enforcement to wrongdoing. In many cases, their willingness to step forward has resulted in important reforms and even saved lives. Congress must encourage employees with reasonable beliefs about criminal activity to report such fraud or abuse by offering meaningful protection to those who blow the whistle rather than leaving them vulnerable to reprisals.

The legislation we introduce today was inspired by a recent report and recommendation from the Government Accountability Office which, based on interviews with key stakeholders, found widespread support for anti-retaliatory protection in criminal antitrust cases. It is modeled on the successful anti-retaliation provisions of the Sarbanes Oxley Act, and is carefully drafted to ensure that whistleblowers have no economic incentive to bring forth false claims.

I have long supported vigorous enforcement of the antitrust laws, which have been called the ''Magna Carta of free enterprise.'' Today's legislation is a necessary complement to them. It has bipartisan support and was recommended by the Government Accountability Office. I urge the Senate to quickly take up and pass this important legislation.

Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

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

S. 3462

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 ''Criminal Antitrust Anti-Retaliation Act''.

SEC. 2. AMENDMENT TO ACPERA.

The Antitrust Criminal Penalty Enhancement and Reform Act of 2004 (Public Law 108–237; 15 U.S.C. 1 note) is amended by adding after section 215 the following:

''SEC. 216. ANTI-RETALIATION PROTECTION FOR WHISTLEBLOWERS.

''(a) WHISTLEBLOWER PROTECTIONS FOR EMPLOYEES, CONTRACTORS, SUBCONTRACTORS, AND AGENTS.—

''(1) IN GENERAL.—No person, or any officer, employee, contractor, subcontractor or agent of such person, may discharge, demote, suspend, threaten, harass, or in any other manner discriminate against a whistleblower in the terms and conditions of employment because—

''(A) the whistleblower provided or caused to be provided to the person or the Federal Government information relating to—

''(i) any violation of, or any act or omission the whistleblower reasonably believes to be a violation of the antitrust laws; or

''(ii) any violation of, or any act or omission the whistleblower reasonably believes to be a violation of another criminal law committed in conjunction with a potential violation of the antitrust laws or in conjunction with an investigation by the Department of Justice of a potential violation of the antitrust laws; or

''(B) the whistleblower filed, caused to be filed, testified, participated in, or otherwise assisted an investigation or a proceeding filed or about to be filed (with any knowledge of the employer) relating to—

''(i) any violation of, or any act or omission the whistleblower reasonably believes to be a violation of the antitrust laws; or

''(ii) any violation of, or any act or omission the whistleblower reasonably believes to be a violation of another criminal law committed in conjunction with a potential violation of the antitrust laws or in conjunction with an investigation by the Department of Justice of a potential violation of the antitrust laws.

''(2) LIMITATION ON PROTECTIONS.—Paragraph (1) shall not apply to any whistleblower if—

''(A) the whistleblower planned and initiated a violation or attempted violation of the antitrust laws;

''(B) the whistleblower planned and initiated a violation or attempted violation of another criminal law in conjunction with a violation or attempted violation of the antitrust laws; or

''(C) the whistleblower planned and initiated an obstruction or attempted obstruction of an investigation by the Department of Justice of a violation of the antitrust laws.

''(3) DEFINITIONS.—In the section:

''(A) PERSON.—The term 'person' has the same meaning as in subsection (a) of the first section of the Clayton Act (15 U.S.C. 12(a)).

''(B) ANTITRUST LAWS.—The term 'antitrust laws' means section 1 or 3 of the Sherman Act (15 U.S.C. 1, 3) or similar State law.

''(C) WHISTLEBLOWER.—The term 'whistleblower' means an employee, contractor, subcontractor, or agent protected from discrimination under paragraph (1).

''(b) ENFORCEMENT ACTION.—

''(1) IN GENERAL.—A whistleblower who alleges discharge or other discrimination by any person 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 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 with the Secretary of Labor 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 the person named in the complaint and to the employer.

''(C) BURDENS OF PROOF.—A complaint filed with the Secretary of Labor under paragraph (1) 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 with the Secretary of Labor not later than 180 days after the date on which the violation occurs.

''(E) CIVIL ACTIONS TO ENFORCE.—If a person fails to comply with an order or preliminary order issued by the Secretary of Labor pursuant to the procedures in section 42121(b), the Secretary of Labor or the person on whose behalf the order was issued may bring a civil action to enforce the order in the district court of the United States for the judicial district in which the violation occurred.

''(c) REMEDIES.—

''(1) IN GENERAL.—A whistleblower prevailing in any action under subsection (b)(1) shall be entitled to all relief necessary to make the whistleblower whole.

''(2) COMPENSATORY DAMAGES.—Relief for any action under paragraph (1) shall include—

''(A) reinstatement with the same seniority status that the whistleblower 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's fees.

''(d) RIGHTS RETAINED BY WHISTLEBLOWERS.—Nothing in this section shall be deemed to diminish the rights, privileges, or remedies of any whistleblower under any Federal or State law, or under any collective bargaining agreement.''.

By Mr. FRANKEN (for himself, Mr. LUGAR, Mr. ROCKEFELLER, Ms. COLLINS, Mrs. SHAHEEN, Mr. WYDEN, Mr. BLUMENTHAL, and Mr. BROWN of Ohio):

S. 3463. A bill to amend title XVIII of the Social Security Act to reduce the incidence of diabetes among Medicare beneficiaries; to the Committee on Finance.

Mr. ROCKEFELLER. Mr. President, I am pleased to join today with my colleagues, Senator FRANKEN, Senator LUGAR, Senator COLLINS, Senator SHAHEEN, Senator WYDEN, Senator BLUMENTHAL, and Senator BROWN of Ohio, to introduce an important piece of bipartisan legislation, the Medicare Diabetes Prevention Act of 2012. Our legislation makes a wise investment in seniors' health by extending the proven

success of the National Diabetes Prevention Program to Medicare. Nearly 26 million American adults have diabetes, and if this disturbing trend doesn't stop, over half of the adult population will either have Type 2 diabetes or its precursor, ''prediabetes,'' by 2020.

Sadly, my home State of West Virginia has one of the highest diabetes rates in the Nation. In 2009, approximately 174,000 adults, which is 11 percent of West Virginia adults, had diabetes. According to Centers for Disease Control estimates, as many as 50 percent of the nearly 380,000 people with Medicare in West Virginia may be at risk of developing this serious, but preventable, illness. If current trends continue, one in three children born in West Virginia after the year 2000 will develop diabetes within his or her lifetime and people with diabetes risk developing terrible complications down the road, including heart disease, stroke, blindness, and amputations.

Diabetes is also one of the main cost drivers in our health care system. The direct economic burden of diabetes was $116 billion for medical expenses and indirect costs totaled $58 billion due to disability, work loss, or premature death in 2007. The costs associated with this preventable disease for Medicare beneficiaries are expected to grow to $2 trillion over the 2011 to 2020 period.

We simply cannot stand idly by in the face of such overwhelming statistics—and fortunately, there is a way to prevent Type 2 diabetes. The National Diabetes Prevention Program, NDPP, is an innovative approach that has demonstrated its effects in preventing the onset of Type 2 diabetes. The NDPP is a proven, community-based intervention that focuses on changing lifestyle behaviors of prediabetic overweight or obese adults through activities that improve dietary choices and increase physical activity in a group setting. In a large-scale clinical trial that has been replicated in community settings, NDPP successfully reduced the onset of diabetes by 58 percent overall and 71 percent in adults over 60.

Because of the impressive success of the National Diabetes Prevention Program, I believe our seniors should have access to its benefits. The Medicare Diabetes Prevention Act of 2012 will help seniors prevent Type 2 diabetes by allowing Medicare to provide the National Diabetes Prevention Program through community settings like the YMCA, local health departments, or even the local church, reaching people with Medicare wherever they live. In the past, physicians have had few tools for their patients who are found to be at risk of diabetes. Under this bill, if a senior is found at risk for diabetes, for example, through their annual wellness visit, their doctor will be able to refer them to an NDPP program in their area.

Unlike Medicare, which needs a Federal legislative change to cover this program, State Medicaid programs already have the authority to pay for this innovative initiative, and it is my hope that more states will do so. By 2020, Medicaid is expected to cover 13 million people with diabetes and about 9 million people who may have pre-diabetes, and states will spend an estimated $83 billion on individuals with diabetes or pre-diabetes. The National Diabetes Prevention program presents an opportunity for States to reduce the incidence of diabetes among individuals enrolled in their Medicaid programs, an especially strategic investment when combined with the expansion of the Medicaid program under health reform.

The coverage of proven solutions under Medicare is nothing new. Yet, rather than providing a traditional drug or procedure, NDPP allows at-risk individuals to change their lifestyles through a community intervention. Implementing NDPP is a unique response to the alarming and escalating rates of diabetes. This public health solution has demonstrated tangible results that can enable our country to prevent diabetes, while reducing health care costs. The NDPP is a strategic and cost-effective intervention that costs less than $500 per person to deliver, compared to the estimated $15,000 per year spent on each Medicare beneficiary with diabetes. According to the Urban Institute, implementing the NDPP nationally could save $191 billion over the next 10 years, with 75 percent of the savings, $142.9 billion, going to the Medicare and Medicaid programs.

Better yet, the National Diabetes Prevention Program is a job creator, bringing diabetes trainers to more communities nationwide to provide the program. West Virginia has already received funding from the Centers for Disease Control and Prevention through a Community Transformation Grant that will allow the State to train at least 100 community health workers to help disseminate the Diabetes Prevention Program in the State over the next 5 years.

The Medicare Diabetes Prevention Act has been endorsed by the American Diabetes Association, American Heart Association, American Public Health Association, National Association of Chronic Disease Directors, National Association of State Long-Term Care Ombudsman Programs, National Council on Aging, Novo Nordisk, Trust for America's Health, the YMCA of the USA, and State YMCA affiliates in over 45 States. With so many Americans at risk for developing diabetes and its potentially severe complications, today is the right time for Medicare to extend the proven National Diabetes Prevention Program as a covered benefit to seniors.

I urge my colleagues to support this timely and important piece of legislation.

By Mr. JOHNSON of South Dakota:

S. 3464. A bill to amend the Mni Wiconi Project Act of 1988 to facilitate completion of the Mni Wiconi Rural Water Supply System, and for other purposes; to the Committee on Energy and Natural Resources.

Mr. JOHNSON of South Dakota. Mr. President, today I introduced legislation to facilitate completion of the Mni Wiconi Rural Water System. The Mni Wiconi Project provides quality drinking water to three Indian Reservations and a non-tribal rural water system in western South Dakota that have historically faced insufficient and, in too many cases, unsafe drinking water.

I have been involved with this project for the entirety of my 25 year congressional career, including sponsoring authorizing legislation that was ultimately enacted in 1988. In authorizing the project, Congress found that the United States has a trust responsibility to ensure that adequate and safe water supplies are available to meet the economic, environmental, water supply, and public health needs of the Pine Ridge Indian Reservation, Rosebud Indian Reservation, and Lower Brule Indian Reservation. With treated drinking water from the Missouri River now reaching most of the three reservations, as well as the 7 county area of the West River/Lyman-Jones Rural Water System, we are very close to completing this critically important project.

Unfortunately, appropriations have failed to keep pace with projected timelines, and additional costs have cut into construction funding. Accordingly, the project requires an increase in the cost ceiling and extension of its authorization in order to be completed and serve the design population. Without an adjustment to the cost ceiling, some portions of the Oglala Sioux Rural Water Supply System and Rosebud Sioux Rural Water System will remain incomplete. The legislation I have introduced today addresses this shortfall and other important aspects of the project. The legislation also directs other Federal agencies that support rural water development to assist the Bureau of Reclamation in improving and repairing existing community water systems that are important components of the project.

Our Federal responsibility to address the tremendous need for adequate and safe drinking water supplies on the Pine Ridge, Rosebud and Lower Brule Indian Reservations remains as important today as it was 25 years ago. I look forward to working with my colleagues to advance this modest but important legislation.

SUBMITTED RESOLUTIONS

SENATE RESOLUTION 534—CONGRATULATING THE NAVY DENTAL CORPS ON ITS 100TH ANNIVERSARY

Mr. MANCHIN submitted the following resolution; which was referred to the Committee on Armed Services:

S. RES. 534

Whereas on August 22, 1912, Congress passed an Act recognizing Navy dentistry as a distinct branch among naval medical professions;

Whereas throughout history, the Navy Dental Corps has supported the Navy by sustaining sailor and marine readiness and providing routine and emergency dental care, ashore and afloat, in peace and in war;

Whereas the Navy Dental Corps works continuously to improve the health of sailors, marines, and their families by supporting individual and community prevention initiatives, good oral hygiene practices, and treatment;

Whereas the Navy Dental Corps endeavors to improve oral health worldwide by participating in the spectrum of military combat, peacekeeping, and humanitarian operations and exercises;

Whereas the Navy Dental Corps, in collaboration with national and international dental organizations, promotes dental professionalism and quality of care;

Whereas the Navy Dental Corps supports the mission of the Federal dental research program and endorses improved dental technologies and therapies through research and adherence to sound scientific principles; and

Whereas the Navy Dental Corps recognizes the importance of continuing professional dental education, requiring and supporting specialty dental education and postgraduate residencies and fellowships for its members: Now, therefore, be it

Resolved, That the Senate—

(1) congratulates the Navy Dental Corps on its 100th anniversary;

(2) commends the Navy Dental Corps for working to sustain the dental readiness and the oral health of a superb fighting force; and

(3) recognizes the thousands of dentists who have served in the Navy Dental Corps over the last 100 years, providing dental care to millions of members of the Armed Forces and their families.

AMENDMENTS SUBMITTED AND PROPOSED

SA 2665. Mr. JOHNSON of Wisconsin submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table.

SA 2666. Mr. JOHNSON of Wisconsin submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2667. Mr. JOHNSON of Wisconsin submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2668. Mr. RUBIO (for himself, Mrs. MCCASKILL, Mr. TOOMEY, Mr. BARRASSO, Ms. AYOTTE, Mrs. SHAHEEN, and Mr. UDALL of New Mexico) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2669. Mr. RUBIO submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2670. Mr. RUBIO submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2671. Mr. RUBIO submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2672. Mr. BROWN of Massachusetts submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2673. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2674. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2675. Ms. MURKOWSKI submitted an amendment intended to be proposed to amendment SA 2645 submitted by Mr. BINGAMAN and intended to be proposed to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2676. Ms. MURKOWSKI submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2677. Mr. WHITEHOUSE (for himself and Ms. MIKULSKI) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2678. Mr. WHITEHOUSE (for himself and Ms. MIKULSKI) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2679. Mr. WHITEHOUSE (for himself and Ms. MIKULSKI) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2680. Mr. WYDEN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2681. Mr. WYDEN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2682. Mr. COBURN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2683. Mr. COBURN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2684. Mr. MCCONNELL (for himself, Mr. HATCH, Mr. KYL, Mr. HOEVEN, Mr. RUBIO, Mrs. HUTCHISON, Mr. ROBERTS, Mr. VITTER, Mr. GRASSLEY, Mr. BARRASSO , Mr. COBURN, Mr. COATS, Mr. INHOFE, Mr. WICKER , and Mr. JOHANNS) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2685. Mrs. GILLIBRAND submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2686. Mrs. GILLIBRAND (for herself and Mr. BENNET) submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2687. Mrs. GILLIBRAND submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2688. Mr. WYDEN (for himself and Mr. KIRK) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2689. Mr. BENNET (for himself and Mr. COBURN) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2690. Ms. MURKOWSKI submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2691. Mrs. HUTCHISON submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2692. Mrs. HUTCHISON (for herself, Mr. MCCAIN, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2693. Mr. COATS submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2694. Mr. COATS submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2695. Mr. SESSIONS submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2696. Mr. MCCAIN (for himself, Mrs. HUTCHISON, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2697. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2698. Mr. PORTMAN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2699. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2700. Mr. ROCKEFELLER (for himself, Mrs. FEINSTEIN, and Mr. PRYOR) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2701. Mr. FRANKEN (for himself, Mr. PAUL, Mr. WYDEN, Mr. AKAKA, Mr. COONS, Mr. BLUMENTHAL, Mr. SANDERS, Mr. UDALL of New Mexico, Mr. MERKLEY, Mr. SCHUMER, Ms. CANTWELL, Mrs. SHAHEEN, Mr. BEGICH, Mr. DURBIN, and Mr. HARKIN) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2702. Mr. FRANKEN (for himself, Mr. PAUL, Mr. WYDEN, Mr. AKAKA, Mr. COONS, Mr. BLUMENTHAL, Mr. SANDERS, Mr. UDALL of New Mexico, Mr. MERKLEY, Mr. SCHUMER, Ms. CANTWELL, Mrs. SHAHEEN, Mr. BEGICH, Mr. DURBIN, and Mr. HARKIN) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2703. Mr. FRANKEN (for himself, Mr. PAUL, Mr. WYDEN, Mr. AKAKA, Mr. COONS, Mr. BLUMENTHAL, Mr. SANDERS, Mr. UDALL of New Mexico, Mr. MERKLEY, Mr. SCHUMER, Ms. CANTWELL, Mrs. SHAHEEN, Mr. BEGICH, Mr. DURBIN, and Mr. HARKIN) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2704. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2705. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2706. Mrs. MURRAY submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2707. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2708. Ms. CANTWELL submitted an amendment intended to be proposed by her

to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2709. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2710. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2711. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2712. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2713. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2714. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2715. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2716. Mr. LEE submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2717. Mrs. SHAHEEN submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2718. Mrs. SHAHEEN submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2719. Mr. KOHL (for himself, Mr. WHITEHOUSE, and Mr. COONS) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2720. Mrs. MCCASKILL submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2721. Mrs. MCCASKILL submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2722. Mrs. MCCASKILL submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2723. Mr. PRYOR submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2724. Ms. MIKULSKI submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2725. Mr. LEE submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2726. Mr. PRYOR submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2727. Mr. BLUMENTHAL (for himself, Mr. SCHUMER, Ms. KLOBUCHAR, Mr. WYDEN, Mr. AKAKA, Mr. SANDERS, and Mrs. SHAHEEN) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2728. Mr. BLUMENTHAL submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2729. Mr. WARNER (for himself and Ms. SNOWE) submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2730. Mr. THUNE submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2731. Mr. REID (for Mr. LIEBERMAN (for himself, Ms. COLLINS, Mr. ROCKEFELLER, Mrs. FEINSTEIN, and Mr. CARPER)) proposed an amendment to the bill S. 3414, supra.

SA 2732. Mr. REID (for Mr. FRANKEN) proposed an amendment to amendment SA 2731 proposed by Mr. REID (for Mr. LIEBERMAN (for himself, Ms. COLLINS, Mr. ROCKEFELLER, Mrs. FEINSTEIN, and Mr. CARPER)) to the bill S. 3414, supra.

SA 2733. Mr. REID proposed an amendment to the bill S. 3414, supra.

SA 2734. Mr. REID proposed an amendment to amendment SA 2733 proposed by Mr. REID to the bill S. 3414, supra.

SA 2735. Mr. REID proposed an amendment to the bill S. 3414, supra.

SA 2736. Mr. REID proposed an amendment to amendment SA 2735 proposed by Mr. REID to the bill S. 3414, supra.

SA 2737. Mr. REID proposed an amendment to amendment SA 2736 proposed by Mr. REID to the amendment SA 2735 proposed by Mr. REID to the bill S. 3414, supra.

SA 2738. Ms. SNOWE (for herself and Mr. WARNER) submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2739. Mrs. GILLIBRAND (for herself and Mr. BENNET) submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2740. Mr. LIEBERMAN (for Mr. NELSON of Florida) proposed an amendment to the resolution S. Res. 525, honoring the life and legacy of Oswaldo Paya Sardinas.

SA 2741. Mr. BLUMENTHAL submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table.

SA 2742. Mr. TESTER submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

TEXT OF AMENDMENTS

SA 2665. Mr. JOHNSON of Wisconsin submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. LIMITATION ON REGULATIONS.

(a) IN GENERAL.—The head of a Federal agency may not issue regulations, standards, or practices that are applicable to the private sector under this Act or an amendment made by this Act until after the date on which the Comptroller General of the United States submits to Congress a report stating that the information infrastructure of the Federal agency is in compliance with the regulations, standards, or practices.

(b) GAO REVIEW.—Upon request by the head of a Federal agency, the Comptroller General of the United States shall—

(1) review the information infrastructure of the Federal agency to determine whether the information infrastructure is in compliance with proposed regulations, standards, or practices; and

(2) submit to Congress a report regarding the conclusion of the review under paragraph (1).

SA 2666. Mr. JOHNSON of Wisconsin submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 8, after line 22, insert the following:

SEC. 3. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b)(2), this Act and the amendments made by this Act shall not take effect until 60 days after the date on which the Congressional Budget Office submits to Congress a report regarding the budgetary effects of this Act.

(b) CBO SCORE.—

(1) REPORT.—The Congressional Budget Office shall submit to Congress a report regarding the budgetary effects of this Act.

(2) EFFECTIVE DATE.—Paragraph (1) shall take effect on the date of enactment of this Act

(c) PUBLIC HEARINGS.—Not later than 60 days after the date on which the Congressional Budget Office submits the report described in subsection (b)(1) to Congress, the head of each agency with responsibility for regulating the security of critical infrastructure under this Act shall hold a public hearing to allow members of the public and industry to comment on the impact of the budgetary effects of this Act.

SA 2667. Mr. JOHNSON of Wisconsin submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 8, after line 22, insert the following:

SEC. 3. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b)(2), this Act and the amendments made by this Act shall not take effect until—

(1) the date on which the Congressional Budget Office submits to Congress a report regarding the budgetary effects of this Act; or

(2) if the report regarding the budgetary effects submitted under subsection (b)(1) determines that the cost of this Act is more than $100,000,000, 60 days after the date on which the determination is published in the Federal Register under subsection (b)(1)(B).

(b) CBO SCORE.—

(1) REPORT.—The Congressional Budget Office shall—

(A) submit to Congress a report regarding the budgetary effects of this Act; and

(B) if the report regarding the budgetary effects described in subparagraph (A) determines that the cost of this Act is more than $100,000,000, publish such determination in the Federal Register and allow public comment during the 60-day period beginning on the date on which such determination is published.

(2) EFFECTIVE DATE.—Paragraph (1) shall take effect on the date of enactment of this Act.

SA 2668. Mr. RUBIO (for himself, Mrs. MCCASKILL, Mr. TOOMEY, Mr. BARRASSO, Ms. AYOTTE, Mrs. SHAHEEN, and Mr. UDALL of New Mexico) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance

the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 165, line 21, strike ''of the United States, including'' and all that follows through line 23 and insert the following:
of the United States.

(b) ADDITIONAL SENSE OF CONGRESS.—

(1) FINDINGS.—Congress finds the following:

(A) Given the importance of the Internet to the global economy, it is essential that the Internet remain stable, secure, and free from government control.

(B) The world deserves the access to knowledge, services, commerce, and communication, the accompanying benefits to economic development, education, and health care, and the informed discussion that is the bedrock of democratic self-government that the Internet provides.

(C) The structure of Internet governance has profound implications for competition and trade, democratization, free expression, and access to information.

(D) Countries have obligations to protect human rights, which are advanced by online activity as well as offline activity.

(E) The ability to innovate, develop technical capacity, grasp economic opportunities, and promote freedom of expression online is best realized in cooperation with all stakeholders.

(F) Proposals have been put forward for consideration at the 2012 World Conference on International Telecommunications that would fundamentally alter the governance and operation of the Internet.

(G) The proposals, in international bodies such as the United Nations General Assembly, the United Nations Commission on Science and Technology for Development, and the International Telecommunication Union, would attempt to justify increased government control over the Internet and would undermine the current multistakeholder model that has enabled the Internet to flourish and under which the private sector, civil society, academia, and individual users play an important role in charting its direction.

(H) The proposals would diminish the freedom of expression on the Internet in favor of government control over content.

(I) The position of the United States Government has been and is to advocate for the flow of information free from government control.

(J) This and past Administrations have made a strong commitment to the multistakeholder model of Internet governance and the promotion of the global benefits of the Internet.

(2) SENSE OF CONGRESS.—It is the sense of Congress that the Secretary of State, in consultation with the Secretary of Commerce, should continue working to implement the position of the United States on Internet governance that clearly articulates the consistent and unequivocal policy of the United States to promote a global Internet free from government control and preserve and advance the successful multistakeholder model that governs the Internet today.

SA 2669. Mr. RUBIO submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 154, strike line 9 and all that follows through page 156, line 13.

SA 2670. Mr. RUBIO submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Strike paragraph (10) of section 707(a).

SA 2671. Mr. RUBIO submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 124, strike line 7 and all that follows through page 128, line 14.

SA 2672. Mr. BROWN of Massachusetts submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 115, between lines 8 and 9, insert the following:

''(10) assist the development and demonstration of technologies designed to increase the security and resiliency of the electricity transmission and distribution grid;

SA 2673. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. CAPPING AND REDUCING THE BALANCE SHEET OF THE FEDERAL RESERVE SYSTEM.

(a) IN GENERAL.—Notwithstanding any other provision of law, no action may be taken by the Board of Governors of the Federal Reserve System or the Federal Open Market Committee on or after the date of enactment of this Act that would result in the total of the factors affecting reserve balances of depository institutions exceeding the balance as of July 27, 2012.

(b) SENSE OF CONGRESS.—It is the sense of Congress that the Federal Reserve System should expeditiously take substantial steps to reduce the size of its balance sheet to levels below those that prevailed prior to the financial crisis of 2008.

SA 2674. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. REPEAL OF DODD-FRANK ACT.

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Public Law 111–203) is repealed, and the provisions of law amended by such Act are revived or restored as if such Act had not been enacted.

SA 2675. Ms. MURKOWSKI submitted an amendment intended to be proposed to amendment SA 2645 submitted by Mr. BINGAMAN and intended to be proposed to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

In lieu of the matter proposed to be inserted, insert the following:

SEC. ___. EMERGENCY AUTHORITY RELATING TO CYBER SECURITY THREATS.

Part II of the Federal Power Act (16 U.S.C. 824 et seq.) is amended by adding at the end the following:

''SEC. 224. EMERGENCY AUTHORITY RELATING TO CYBER SECURITY THREATS.

''(a) DEFINITIONS.—In this section:

''(1) CRITICAL ELECTRIC INFRASTRUCTURE.—The term 'critical electric infrastructure' means systems and assets, whether physical or virtual, used for the generation, transmission, or distribution of electric energy affecting interstate commerce that, as determined by the Commission or the Secretary (as appropriate), are so vital to the United States that the incapacity or destruction of the systems and assets would have a debilitating impact on national security, national economic security, or national public health or safety.

''(2) CYBER SECURITY THREAT.—The term 'cyber security threat' means the imminent danger of an act that disrupts, attempts to disrupt, or poses a significant risk of disrupting the operation of programmable electronic devices or communications networks (including hardware, software, and data) essential to the reliable operation of critical electric infrastructure.

''(3) SECRETARY.—The term 'Secretary' means the Secretary of Energy.

''(b) EMERGENCY AUTHORITY OF SECRETARY.—

''(1) IN GENERAL.—If the Secretary determines that immediate action is necessary to protect critical electric infrastructure from a cyber security threat, the Secretary may require, by order, with or without notice, persons subject to the jurisdiction of the Commission to take such actions as the Secretary determines will best avert or mitigate the cyber security threat.

''(2) COORDINATION WITH CANADA AND MEXICO.—In exercising the authority granted under this subsection, the Secretary is encouraged to consult and coordinate with the appropriate officials in Canada and Mexico responsible for the protection of cyber security of the interconnected North American electricity grid.

''(3) CONSULTATION.—Before exercising the authority granted under this subsection, to the extent practicable, taking into account the nature of the threat and urgency of need for action, the Secretary shall consult with any entity that owns, controls, or operates critical electric infrastructure and with officials at other Federal agencies, as appropriate, regarding implementation of actions that will effectively address the identified cyber security threat.

''(4) COST RECOVERY.—The Commission shall establish a mechanism that permits public utilities to recover prudently incurred costs required to implement immediate actions ordered by the Secretary under this subsection.

''(c) DURATION OF EXPEDITED OR EMERGENCY RULES OR ORDERS.—Any order issued by the Secretary under subsection (b) shall remain effective for not more than 90 days unless, during the 90 day-period, the Secretary—

''(1) gives interested persons an opportunity to submit written data, views, or arguments; and

''(2) affirms, amends, or repeals the rule or order.''.

SA 2676. Ms. MURKOWSKI submitted an amendment intended to be proposed

by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 153, strike line 15 and all that follows through page 154, line 8, and insert the following:

SEC. 414. REPORT ON PROTECTING THE ELECTRICAL GRID OF THE UNITED STATES.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary of Energy, in consultation with the Federal Energy Regulatory Commission, the Secretary, the Director of National Intelligence, and the electric sector coordinating council shall submit to Congress a report on—

(1) the threat of a cyber attack disrupting the electrical grid of the United States;

(2) the existing standards, alerts, and mitigation strategies in place;

(3) the implications for the national security of the United States if the electrical grid is disrupted;

(4)(A) the interdependency of critical infrastructures; and

(B) the options available to the United States and private sector entities to reconstitute—

(i) as soon as practicable after the disruption, electrical service to provide for the national security of the United States; and

(ii) within a reasonable time frame after the disruption, all electrical service within the United States; and

(5) a plan, building on existing efforts, to prevent disruption of the electric grid of the United States caused by a cyber attack.

(b) REQUIREMENTS.—In preparing the report under subsection (a), the Secretary of Energy shall use any existing studies or reports to avoid duplication of effort.

SA 2677. Mr. WHITEHOUSE (for himself and Ms. MIKULSKI) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 166, line 19, strike ''coordinate'' and insert ''collaborate''.

On page 166, line 23, strike ''to develop'' and insert ''on''.

On page 166, beginning on line 24, strike ''cyberspace, cybersecurity, and cybercrime issues'' and insert ''cyber issues''.

On page 167, line 11, after ''State'' insert ''and the Attorney General''.

On page 168, line 15, after ''State'' insert ''and the Attorney General''.

On page 168, line 17, after ''State'' insert ''and the Attorney General''.

SA 2678. Mr. WHITEHOUSE (for himself and Ms. MIKULSKI) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 91, between lines 12 and 13, insert the following:

''(16) PROTECT.—The term 'protect' means the action of securing, defending, or reducing the vulnerabilities of an information system, or otherwise enhancing information security or the resiliency of information systems or assets.

''(17) PROTECTION.—The term 'protection' means the actions undertaken to secure, defend, or reduce the vulnerabilities of an information system, or otherwise enhance information security or the resiliency of information systems or assets.

''(18) RESPOND AND RESPONSE.—The terms 'respond' and 'response' in relation to cybersecurity threats, vulnerabilities, or incidents do not include directing cybersecurity threat and incident law enforcement investigations or prosecutions.

On page 95, line 10, strike ''security'' and insert ''protection''.

On page 99, after line 25, insert the following:

''(m) LAW ENFORCEMENT AND INTELLIGENCE AUTHORITIES.—Nothing in this section shall be construed to alter or amend the law enforcement or intelligence authorities of any Federal agency.

SA 2679. Mr. WHITEHOUSE (for himself and Ms. MIKULSKI) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title IV, add the following:

SEC. 416. REPORT ON FEDERAL LAW ENFORCEMENT CYBERSECURITY AND CYBERCRIME RESOURCES.

(a) DEFINITIONS.—In this section—

(1) the term ''covered law enforcement agency'' means each law enforcement component of—

(A) the Department of Justice; and

(B) the Department of Homeland Security; and

(2) the term ''mission'' means the portion of a cybersecurity mission that encompasses law enforcement and intelligence activities.

(b) REPORT.—

(1) IN GENERAL.—The Attorney General shall enter into a contract with the National Research Council, or another federally funded research and development corporation, under which the National Research Council or other corporation shall submit to Congress a report on the current and optimal level and structure of cybersecurity and cybercrime resources of each covered law enforcement agency.

(2) CONTENTS.—The report described in paragraph (1) shall—

(A) identify the elements of the mission of each covered law enforcement agency;

(B) describe the challenges involved in the mission of each covered law enforcement agency, including—

(i) any challenges in cybercrime prosecutions, such as the need for advanced forensics expertise and resources;

(ii) the complexity of relevant Federal laws, State laws, international laws, and treaty obligations of the United States;

(iii) the need to coordinate with members of the intelligence community;

(iv) the need to protect classified or sensitive information while abiding by relevant law regarding the disclosure of exculpatory evidence and other discoverable information to a criminal defendant; and

(v) any other challenges that the report may identify;

(C) identify the current resources brought to bear by each covered law enforcement agency in pursuing the mission of that agency, differentiating between—

(i)(I) personnel who focus exclusively on supporting the mission; and

(II) personnel who hold multiple or competing responsibilities;

(ii)(I) operational personnel; and

(II) personnel who hold primarily management, policy making, or support responsibilities;

(iii)(I) personnel working at headquarters; and

(II) personnel working in the field; and

(iv)(I) personnel with specialized training and duties relating to national cybersecurity; and

(II) personnel with general technical training;

(D) identify areas in which the level and structure of current resources is inadequate for any covered law enforcement agency to perform the mission of that agency;

(E) identify the optimal level of resources that would enable each covered law enforcement agency to perform the mission of that agency most effectively without unnecessary government waste;

(F) identify the optimal structure of the cybersecurity and cybercrime resources of each covered law enforcement agency, considering existing models within—

(i) the Department of Justice, including task forces and strike forces; and

(ii) agencies such as the Drug Enforcement Administration and the Bureau of Alcohol, Tobacco, Firearms, and Explosives; and

(G) evaluate the future or developing needs of each covered law enforcement agency, including the resources that the agency will need to perform the mission of that agency in the future.

(3) TIMING.—The contract entered into under paragraph (1) shall require that the report described in this subsection be submitted not later than 1 year after the date of enactment of this Act.

SA 2680. Mr. WYDEN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title VI, insert the following:

SEC. 606. RULE OF CONSTRUCTION.

Nothing in this Act may be construed as authorizing the President to enter the United States into a treaty or binding international agreement on cybersecurity unless such treaty or agreement is approved with the advice and consent of the Senate pursuant to Article II, section 2, clause 2 of the Constitution.

SA 2681. Mr. WYDEN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 46, strike line 6 and all that follows through page 57, line 3, and insert the following:

''(4) provide a mechanism to improve and continuously monitor the security of agency information security programs and systems, subject to the protection of the privacy of individual or customer-specific data, through a focus on continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

''SEC. 3552. DEFINITIONS.

''(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 (including the definitions of the terms 'agency' and 'information system') shall apply to this subchapter.

''(b) OTHER TERMS.—In this subchapter:

''(1) ADEQUATE SECURITY.—The term 'adequate security' means security commensurate with the risk and impact resulting from the unauthorized access to or loss, misuse, destruction, or modification of information.

''(2) CONTINUOUS MONITORING.—The term 'continuous monitoring' means the ongoing real time or near real time process used to determine if the complete set of planned, required, and deployed security controls within an agency information system continue to be effective over time in light of rapidly changing information technology and threat development. To the maximum extent possible, subject to the protection of the privacy of individual or customer-specific data, this also requires automation of that process to enable cost effective, efficient, and consistent monitoring and provide a more dynamic view of the security state of those deployed controls.

''(3) COUNTERMEASURE.—The term 'countermeasure' means automated or manual actions with defensive intent to modify or block data packets associated with electronic or wire communications, Internet traffic, program code, or other system traffic transiting to or from or stored on an information system for the purpose of protecting the information system from cybersecurity threats, conducted on an information system owned or operated by or on behalf of the party to be protected or operated by a private entity acting as a provider of electronic communication services, remote computing services, or cybersecurity services to the party to be protected.

''(4) INCIDENT.—The term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of agency information or an agency information system; or

''(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

''(5) INFORMATION SECURITY.—The term 'information security' means protecting agency information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

''(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring nonrepudiation and authenticity;

''(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

''(C) availability, which means ensuring timely and reliable access to and use of information.

''(6) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given that term in section 11101 of title 40.

''(7) NATIONAL SECURITY SYSTEM.—

''(A) IN GENERAL.—The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) that is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(B) EXCLUSION.—Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

''(8) SECRETARY.—The term 'Secretary' means the Secretary of Homeland Security.

''SEC. 3553. FEDERAL INFORMATION SECURITY AUTHORITY AND COORDINATION.

''(a) IN GENERAL.—Except as provided in subsections (f) and (g), the Secretary shall oversee agency information security policies and practices, including the development and oversight of information security policies and directives and compliance with this subchapter.

''(b) DUTIES.—The Secretary shall—

''(1) develop, issue, and oversee the implementation of information security policies and directives, which shall be compulsory and binding on agencies to the extent determined appropriate by the Secretary, including—

''(A) policies and directives consistent with the standards promulgated under section 11331 of title 40 to identify and provide information security protections that are commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected, created, processed, stored, disseminated, or otherwise used or maintained by or on behalf of an agency; or

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization, such as a State government entity, on behalf of an agency;

''(B) minimum operational requirements for network operations centers and security operations centers of agencies to facilitate the protection of and provide common situational awareness for all agency information and information systems;

''(C) reporting requirements, consistent with relevant law, regarding information security incidents;

''(D) requirements for agencywide information security programs, including continuous monitoring of agency information systems;

''(E) performance requirements and metrics for the security of agency information systems;

''(F) training requirements to ensure that agencies are able to fully and timely comply with directions issued by the Secretary under this subchapter;

''(G) training requirements regarding privacy, civil rights, civil liberties, and information oversight for agency information security employees;

''(H) requirements for the annual reports to the Secretary under section 3554(c); and

''(I) any other information security requirements as determined by the Secretary;

''(2) review agency information security programs required to be developed under section 3554(b);

''(3) develop and conduct targeted risk assessments and operational evaluations for agency information and information systems in consultation with the heads of other agencies or governmental and private entities that own and operate such systems, that may include threat, vulnerability, and impact assessments and penetration testing;

''(4) operate consolidated intrusion detection, prevention, or other protective capabilities and use associated countermeasures for the purpose of protecting agency information and information systems from information security threats;

''(5) in conjunction with other agencies and the private sector, assess and foster the development of information security technologies and capabilities for use across multiple agencies;

''(6) designate an entity to receive reports and information about information security incidents, threats, and vulnerabilities affecting agency information systems;

''(7) provide incident detection, analysis, mitigation, and response information and remote or on-site technical assistance to the heads of agencies;

''(8) coordinate with appropriate agencies and officials to ensure, to the maximum extent feasible, that policies and directives issued under paragraph (1) are complementary with—

''(A) standards and guidelines developed for national security systems; and

''(B) policies and directives issues by the Secretary of Defense, Director of the Central Intelligence Agency, and Director of National Intelligence under subsection (g)(1);

''(9) not later than March 1 of each year, submit to Congress a report on agency compliance with the requirements of this subchapter, which shall include—

''(A) a summary of the incidents described by the reports required in section 3554(c);

''(B) a summary of the results of assessments required by section 3555;

''(C) a summary of the results of evaluations required by section 3556;

''(D) significant deficiencies in agency information security practices as identified in the reports, assessments, and evaluations referred to in subparagraphs (A), (B), and (C), or otherwise; and

''(E) planned remedial action to address any deficiencies identified under subparagraph (D); and

''(10) with respect to continuous monitoring reporting, allow operators of agency information systems to use processes that will protect the privacy of individual or nongovernment customer specific data.

''(c) ISSUING POLICIES AND DIRECTIVES.—When issuing policies and directives under subsection (b), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology and issued by the Secretary of Commerce under section 11331 of title 40. The Secretary shall consult with the Director of the National Institute of Standards and Technology when such policies and directives implement standards or guidelines developed by National Institute of Standards and Technology. To the maximum extent feasible, such standards and guidelines shall be complementary with standards and guidelines developed for national security systems.

''(d) COMMUNICATIONS AND SYSTEM TRAFFIC.—

''(1) IN GENERAL.—Notwithstanding any other provision of law, in carrying out the responsibilities under paragraphs (3) and (4) of subsection (b), if the Secretary makes a certification described in paragraph (2), the Secretary may acquire, intercept, retain, use, and disclose communications and other system traffic that are transiting to or from or stored on agency information systems and deploy countermeasures with regard to the communications and system traffic, unless the head of an agency determines within a reasonable time, and reports to the President, that such acquisition, interception, retention, use, or disclosure is contrary to the public interest and would seriously undermine important agency goals, activities, or programs.

''(2) CERTIFICATION.—A certification described in this paragraph is a certification by the Secretary that—

''(A) the acquisitions, interceptions, and countermeasures are reasonably necessary

for the purpose of protecting agency information systems from information security threats;

''(B) the content of communications will be collected and retained only when the communication is associated with a known or reasonably suspected information security threat, and communications and system traffic will not be subject to the operation of a countermeasure unless associated with the threats;

''(C) information obtained under activities authorized under this subsection will only be retained, used, or disclosed to protect agency information systems from information security threats, mitigate against such threats, or, with the approval of the Attorney General, for law enforcement purposes when—

''(i) the information is evidence of a cybersecurity crime that has been, is being, or is about to be committed; and

---

SA 2682. Mr. COBURN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. ANNUAL REPORT ON FOREIGN GOVERNMENT SPONSORS OF ECONOMIC OR INDUSTRIAL ESPIONAGE.

(a) IN GENERAL.—Subject to subsection (c), not later than 180 days after the date of enactment of this Act, and annually thereafter, the National Counterintelligence Executive shall submit to Congress, the President, the National Security Council, the Secretary of State, the Secretary of Defense, the Secretary of the Treasury, and the Secretary of Commerce—

(1) an unclassified report that contains a list of foreign governments that the National Counterintelligence Executive determines engage in, sponsor, or condone economic or industrial espionage against United States businesses or other persons; and

(2) a classified report that includes—

(A) the report submitted under paragraph (1); and

(B) the information upon which the determinations of the National Counterintelligence Executive under paragraph (1) are based.

(b) INFORMATION.—In preparing a report under subsection (a), the National Counterintelligence Executive shall rely primarily on information available to the United States Government.

(c) REVIEW BY SECRETARY OF STATE.—

(1) SUBMISSION OF REPORT FOR REVIEW.—Not later than 30 days before the date on which the National Counterintelligence Executive submits a report required under subsection (a), the National Counterintelligence Executive shall submit the report to the Secretary of State.

(2) FEEDBACK.—The Secretary of State may provide feedback to the National Counterintelligence Executive with respect to a report submitted to the Secretary of State under paragraph (1).

(3) DELAY.—Upon the request of the Secretary of State, the National Counterintelligence Executive shall delay the submission of a report under subsection (a) for a period of not more than 60 days.

SA 2683. Mr. COBURN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title V, add the following:

SEC. 503. DEPARTMENT OF DEFENSE PROVISION FOR THE COMMON DEFENSE OF FEDERAL INFORMATION INFRASTRUCTURE IN FEDERAL CYBER EMERGENCIES.

(a) AUTHORITY FOR PRESIDENT TO DIRECT.—The President shall have the authority to direct the Department of Defense to provide for the common defense of Federal information infrastructure in the event of a Federal cyber emergency.

(b) FEDERAL CYBER EMERGENCY.—For purposes of this section, a Federal cyber emergency is an incident that threatens the viability of Federal information infrastructure necessary for maintaining critical Federal government functions or operations.

(c) SCOPE.—The authorities exercised by the Department of Defense pursuant to subsection (a) may, as directed by the President under that subsection, including the authorities in section 3553 of title 44, United States Code (as amended by section 201 of this Act).

(d) DURATION OF AUTHORITY.—Any direction of the Department of Defense to provide for the common defense of Federal information infrastructure in the event of a Federal cyber emergency under subsection (a) shall be for such period, not to exceed seven days, as the President shall direct under that subsection.

(e) NOTICE TO CONGRESS.—The President shall notify Congress immediately upon directing the Department of Defense to provide for the common defense of Federal information infrastructure under subsection (a), and shall provide daily updates to Congress thereafter until the authority to provide for such defense expires.

(f) CONSTRUCTION.—Nothing in this section shall be construed to grant the Department of Defense authority, jurisdiction, or control over any non-Federal information infrastructure.

SA 2684. Mr. MCCONNELL submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE __—REPEAL OF OBAMACARE

SEC. ___. REPEAL OF OBAMACARE.

(a) FINDINGS.—Congress finds the following with respect to the impact of Public Law 111–148 and related provisions of Public Law 111–152 (collectively referred to in this section as ''the law''):

(1) President Obama promised the American people that if they liked their current health coverage, they could keep it. But even the Obama Administration admits that tens of millions of Americans are at risk of losing their health care coverage, including as many as 8 in 10 plans offered by small businesses.

(2) Despite projected spending of more than two trillion dollars over the next 10 years, cutting Medicare by more than one-half trillion dollars over that period, and increasing taxes by over $800 billion dollars over that period, the law does not lower health care costs. In fact, the law actually makes coverage more expensive for millions of Americans. The average American family already paid a premium increase of approximately $1,200 in the year following passage of the law. The Congressional Budget Office (CBO) predicts that health insurance premiums for individuals buying private health coverage on their own will increase by $2,100 in 2016 compared to what the premiums would have been in 2016 if the law had not passed.

(3) The law cuts more than one-half trillion dollars in Medicare and uses the funds to create a new entitlement program rather than to protect and strengthen the Medicare program. Actuaries at the Centers for Medicare & Medicaid Services (CMS) warn that the Medicare cuts contained in the law are so drastic that ''providers might end their participation in the program (possibly jeopardizing access to care for beneficiaries)''. CBO cautioned that the Medicare cuts ''might be difficult to sustain over a long period of time''. According to the CMS actuaries, 7.4 million Medicare beneficiaries who would have been enrolled in a Medicare Advantage plan in 2017 will lose access to their plan because the law cuts $206 billion in payments to Medicare Advantage plans. The Trustees of the Medicare Trust Funds predict that the law will result in a substantial decline in employer-sponsored retiree drug coverage, and 90 percent of seniors will no longer have access to retiree drug coverage by 2016 as a result of the law.

(4) The law creates a 15-member, unelected Independent Payment Advisory Board that is empowered to make binding decisions regarding what treatments Medicare will cover and how much Medicare will pay for treatments solely to cut spending, restricting access to health care for seniors.

(5) The law and the more than 13,000 pages of related regulations issued before July 11, 2012, are causing great uncertainty, slowing economic growth, and limiting hiring opportunities for the approximately 13 million Americans searching for work. Imposing higher costs on businesses will lead to lower wages, fewer workers, or both.

(6) The law imposes 21 new or higher taxes on American families and businesses, including 12 taxes on families making less than $250,000 a year.

(7) While President Obama promised that nothing in the law would fund elective abortion, the law expands the role of the Federal Government in funding and facilitating abortion and plans that cover abortion. The law appropriates billions of dollars in new funding without explicitly prohibiting the use of these funds for abortion, and it provides Federal subsidies for health plans covering elective abortions. Moreover, the law effectively forces millions of individuals to personally pay a separate abortion premium in violation of their sincerely held religious, ethical, or moral beliefs.

(8) Until enactment of the law, the Federal Government has not sought to impose specific coverage or care requirements that infringe on the rights of conscience of insurers, purchasers of insurance, plan sponsors, beneficiaries, and other stakeholders, such as individual or institutional health care providers. The law creates a new nationwide requirement for health plans to cover ''essential health benefits'' and ''preventive services'', but does not allow stakeholders to opt out of covering items or services to which they have a religious or moral objection, in violation of the Religious Freedom Restoration Act (Public Law 103–141). By creating new barriers to health insurance and causing the loss of existing insurance arrangements, these inflexible mandates jeopardize the ability of institutions and individuals to exercise their rights of conscience and their ability to freely participate in the health insurance and health care marketplace.

(9) The law expands government control over health care, adds trillions of dollars to existing liabilities, drives costs up even further, and too often put Federal bureaucrats, instead of doctors and patients, in charge of health care decisionmaking.

(10) The path to patient-centered care and lower costs for all Americans must begin with a full repeal of the law.

(b) REPEAL.—

(1) PPACA.—Effective as of the enactment of Public Law 111–148, such Act (other than subsection (d) of section 1899A of the Social Security Act, as added and amended by sections 3403 and 10320 of such Public Law) is repealed, and the provisions of law amended or repealed by such Act (other than such subsection (d)) are restored or revived as if such Act had not been enacted.

(2) HEALTH CARE-RELATED PROVISIONS IN THE HEALTH CARE AND EDUCATION RECONCILIATION ACT OF 2010.—Effective as of the enactment of the Health Care and Education Reconciliation Act of 2010 (Public Law 111–152), title I and subtitle B of title II of such Act are repealed, and the provisions of law amended or repealed by such title or subtitle, respectively, are restored or revived as if such title and subtitle had not been enacted.

SEC. ___. BUDGETARY EFFECTS OF THIS ACT.

The budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go Act of 2010, shall be determined by reference to the latest statement titled ''Budgetary Effects of PAYGO Legislation'' for this Act, submitted for printing in the Congressional Record by the Chairman of the Senate Budget Committee, provided that such statement has been submitted prior to the vote on passage.

SA 2685. Mrs. GILLIBRAND submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 110, lines 17 and 18, after ''research laboratories'' insert the following: ''(including the defense laboratories (as defined in section 2199 of title 10, United States Code) and the national laboratories of the Department of Energy)''.

SA 2686. Mrs. GILLIBRAND (for herself and Mr. BENNET) submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title IV, insert the following:

SEC. 416. SENSE OF CONGRESS.

(a) FINDINGS.—Congress finds the following:

(1) A report from the Bipartisan Policy Center's Cyber Security Task Force, published in July 2012, found that—

(A) 50,000 cyber attacks were reported to the Department of Homeland Security between October 2011 and February 2012; and

(B) 86 of the attacks described in subparagraph (A) took place on critical infrastructure networks.

(2) The report of the Commission on Cybersecurity for the 44th President from the Center for Strategic and International Studies (referred to in this subsection as ''CSIS''), published in November 2010, concluded that the United States is facing an imminent crisis in cybersecurity human capital.

(3) The November 2010 CSIS report cited another CSIS report, entitled ''A Human Capital Crisis in Cybersecurity'', which estimated that 1,000 specialists who had the specialized cybersecurity skills needed to defend the United States effectively in cyberspace existed in the United States, but the number of cybersecurity specialists needed that year was between 10,000 and 30,000.

(4) Another report published by CSIS, entitled ''Cybersecurity Two Years Later'', noted that ''there has been slow progress in changing the situation from where we were two years ago''.

(b) SENSE OF CONGRESS.—It is the sense of Congress that, recognizing that the United States is currently facing a human capital crisis in cybersecurity, the President should—

(1) develop model standards, in coordination with any existing standards, for nonprofit institutions that provide training programs to develop advanced technical proficiency for individuals seeking careers in computer network defense;

(2) emphasize experiential learning and the opportunity to take on significant real-world casework as essential parts of training and development programs for cybersecurity professions;

(3) recognize institutions which develop advanced technical proficiency and provide real-world casework for individuals seeking careers in computer network defense as examples of excellence in specialized cybersecurity training;

(4) employ resources to support nonprofit institutions to expand the cybersecurity human capital capacity of the United States, particularly by supporting or establishing education and training programs which—

(A) demonstrate current and projected caseload of sufficient, important system and network defense activity to provide real-world training opportunities for trainees, with a heavy emphasis on real-life, hands-on, high-level cybersecurity work;

(B) demonstrate practical computer network defense skills and up-to-date cybersecurity experience of the senior staff proposing to lead the education and training programs;

(C) demonstrate access to hands-on training programs in the most up-to-date computer network defense technologies and techniques; and

(D) collaborate with the Federal Government and private sector companies in the United States in such programs; and

(5) establish a program recognizing citizens who have demonstrated outstanding leadership and service as mentors in the field of cybersecurity.

SA 2687. Mrs. GILLIBRAND submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of section 301, add the following:

(i) COORDINATION WITH DEPARTMENT OF DEFENSE AND DEPARTMENT OF ENERGY LABORATORIES.—It is the sense of Congress that to avoid duplication of Federal efforts in developing and executing a national cybersecurity research and development plan, the Director should ensure that coordination with other research initiatives under subsection (e) includes coordination with the defense laboratories (as defined in section 2199 of title 10, United States Code) and the national laboratories of the Department of Energy that are addressing challenges similar to the challenges described in subsection (b).

SA 2688. Mr. WYDEN (for himself and Mr. KIRK) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE VIII—GEOLOCATION INFORMATION

SEC. 801. SHORT TITLES.

This title may be cited as the ''Geolocational Privacy and Surveillance Act'' or the ''GPS Act''.

SEC. 802. PROTECTION OF GEOLOCATION INFORMATION.

(a) IN GENERAL.—Part 1 of title 18, United States Code, is amended by inserting after chapter 119 the following:

''CHAPTER 120—GEOLOCATION INFORMATION

''§ 2601. Definitions

''In this chapter:

''(1) COVERED SERVICE.—The term 'covered service' means an electronic communication service, a geolocation information service, or a remote computing service.

''(2) ELECTRONIC COMMUNICATION SERVICE.—The term 'electronic communication service' has the meaning given that term in section 2510.

''(3) ELECTRONIC SURVEILLANCE.—The term 'electronic surveillance' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

''(4) GEOLOCATION INFORMATION.—The term 'geolocation information' means, with respect to a person, any information, that is not the content of a communication, concerning the location of a wireless communication device or tracking device (as that term is defined section 3117) that, in whole or in part, is generated by or derived from the operation of that device and that could be used to determine or infer information regarding the location of the person.

''(5) GEOLOCATION INFORMATION SERVICE.—The term 'geolocation information service' means the provision of a global positioning service or other mapping, locational, or directional information service to the public, or to such class of users as to be effectively available to the public, by or through the operation of any wireless communication device, including any mobile telephone, global positioning system receiving device, mobile computer, or other similar or successor device.

''(6) INTERCEPT.—The term 'intercept' means the acquisition of geolocation information through the use of any electronic, mechanical, or other device.

''(7) INVESTIGATIVE OR LAW ENFORCEMENT OFFICER.—The term 'investigative or law enforcement officer' means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of, or to make arrests for, offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses.

''(8) PERSON.—The term 'person' means any employee or agent of the United States, or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.

''(9) REMOTE COMPUTING SERVICE.—The term 'remote computing service' has the meaning given that term in section 2711.

''(10) STATE.—The term 'State' means any State of the United States, the District of

Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

''(11) WIRELESS COMMUNICATION DEVICE.—The term 'wireless communication device' means any device that enables access to, or use of, an electronic communication system or service or a covered service, if that device utilizes a radio or other wireless connection to access such system or service.

''§ 2602. Interception and disclosure of geolocation information

''(a) IN GENERAL.—

''(1) PROHIBITION ON DISCLOSURE OR USE.—Except as otherwise specifically provided in this chapter, it shall be unlawful for any person to—

''(A) intentionally intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, geolocation information pertaining to another person;

''(B) intentionally disclose, or endeavor to disclose, to any other person geolocation information pertaining to another person, knowing or having reason to know that the information was obtained through the interception of such information in violation of this paragraph;

''(C) intentionally use, or endeavor to use, any geolocation information, knowing or having reason to know that the information was obtained through the interception of such information in violation of this paragraph; or

''(D)(i) intentionally disclose, or endeavor to disclose, to any other person the geolocation information pertaining to another person intercepted by means authorized by subsections (b) through (h), except as provided in such subsections;

''(ii) knowing or having reason to know that the information was obtained through the interception of such information in connection with a criminal investigation;

''(iii) having obtained or received the information in connection with a criminal investigation; and

''(iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation.

''(2) PENALTY.—Any person who violates paragraph (1) shall be fined under this title, imprisoned not more than five years, or both.

''(b) EXCEPTION FOR INFORMATION ACQUIRED IN THE NORMAL COURSE OF BUSINESS.—It shall not be unlawful under this chapter for an officer, employee, or agent of a provider of a covered service, whose facilities are used in the transmission of geolocation information, to intercept, disclose, or use that information in the normal course of the officer, employee, or agent's employment while engaged in any activity which is a necessary incident to the rendition of service or to the protection of the rights or property of the provider of that service, except that a provider of a geolocation information service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

''(c) EXCEPTION FOR CONDUCTING FOREIGN INTELLIGENCE SURVEILLANCE.—Notwithstanding any other provision of this chapter, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of the official duty of the officer, employee, or agent to conduct electronic surveillance, as authorized by the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

''(d) EXCEPTION FOR CONSENT.—

''(1) IN GENERAL.—It shall not be unlawful under this chapter for a person to intercept geolocation information pertaining to another person if such other person has given prior consent to such interception unless such information is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

''(2) CHILDREN.—The exception in paragraph (1) permits a parent or legal guardian of a child to intercept geolocation information pertaining to that child or to give consent for another person to intercept such information.

''(e) EXCEPTION FOR PUBLIC INFORMATION.—It shall not be unlawful under this chapter for any person to intercept or access geolocation information relating to another person through any system that is configured so that such information is readily accessible to the general public.

''(f) EXCEPTION FOR EMERGENCY INFORMATION.—It shall not be unlawful under this chapter for any investigative or law enforcement officer or other emergency responder to intercept or access geolocation information relating to a person if such information is used—

''(1) to respond to a request made by such person for assistance; or

''(2) in circumstances in which it is reasonable to believe that the life or safety of the person is threatened, to assist the person.

''(g) EXCEPTION FOR THEFT OR FRAUD.—It shall not be unlawful under this chapter for a person acting under color of law to intercept geolocation information pertaining to the location of another person who has unlawfully taken the device sending the geolocation information if—

''(1) the owner or operator of such device authorizes the interception of the person's geolocation information;

''(2) the person acting under color of law is lawfully engaged in an investigation; and

''(3) the person acting under color of law has reasonable grounds to believe that the geolocation information of the other person will be relevant to the investigation.

''(h) EXCEPTION FOR WARRANT.—

''(1) DEFINITIONS.—In this subsection:

''(A) COURT OF COMPETENT JURISDICTION.—The term 'court of competent jurisdiction' includes—

''(i) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that—

''(I) has jurisdiction over the offense being investigated;

''(II) is in or for a district in which the provider of a geolocation information service is located or in which the geolocation information is stored; or

''(III) is acting on a request for foreign assistance pursuant to section 3512; or

''(ii) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants.

''(B) GOVERNMENTAL ENTITY.—The term 'governmental entity' means a department or agency of the United States or any State or political subdivision thereof.

''(2) WARRANT.—A governmental entity may intercept geolocation information or require the disclosure by a provider of a covered service of geolocation information 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, or as otherwise provided in this chapter or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

''(i) PROHIBITION ON DIVULGING GEOLOCATION INFORMATION.—

''(1) IN GENERAL.—Except as provided in paragraph (2), a person providing a covered service shall not intentionally divulge geolocation information pertaining to another person.

''(2) EXCEPTIONS.—A person providing a covered service may divulge geolocation information—

''(A) as otherwise authorized in subsections (b) through (h);

''(B) with the lawful consent of such other person;

''(C) to another person employed or authorized, or whose facilities are used, to forward such geolocation information to its destination; or

''(D) which was inadvertently obtained by the provider of the covered service and which appears to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

''§ 2603. Prohibition of use as evidence of acquired geolocation information

''Whenever any geolocation information has been acquired, no part of such information and no evidence derived therefrom may 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 a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

''§ 2604. Emergency situation exception

''(a) EMERGENCY SITUATION EXCEPTION.—Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, may intercept geolocation information if—

''(1) such officer reasonably determines that an emergency situation exists that—

''(A) involves—

''(i) immediate danger of death or serious physical injury to any person;

''(ii) conspiratorial activities threatening the national security interest; or

''(iii) conspiratorial activities characteristic of organized crime; and

''(B) requires geolocation information be intercepted before an order authorizing such interception can, with due diligence, be obtained;

''(2) there are grounds upon which an order could be entered to authorize such interception; and

''(3) an application for an order approving such interception is made within 48 hours after the interception has occurred or begins to occur.

''(b) FAILURE TO OBTAIN COURT ORDER.—

''(1) TERMINATION OF ACQUISITION.—In the absence of an order, an interception of geolocation information carried out under subsection (a) shall immediately terminate when the information sought is obtained or when the application for the order is denied, whichever is earlier.

''(2) PROHIBITION ON USE AS EVIDENCE.—In the event such application for approval is denied, the geolocation information shall be treated as having been obtained in violation of this chapter and an inventory shall be served on the person named in the application.

''§ 2605. Recovery of civil damages authorized

''(a) IN GENERAL.—Any person whose geolocation information is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person, other than the United States, which engaged in that violation such relief as may be appropriate.

''(b) RELIEF.—In an action under this section, appropriate relief includes—

''(1) such preliminary and other equitable or declaratory relief as may be appropriate;

''(2) damages under subsection (c) and punitive damages in appropriate cases; and

''(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

''(c) COMPUTATION OF DAMAGES.—The court may assess as damages under this section whichever is the greater of—

''(1) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

''(2) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

''(d) DEFENSE.—It is a complete defense against any civil or criminal action brought against an individual for conduct in violation of this chapter if such individual acted in a good faith reliance on—

''(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

''(2) a request of an investigative or law enforcement officer under section 2604; or

''(3) a good-faith determination that an exception under section 2602 permitted the conduct complained of.

''(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

''(f) ADMINISTRATIVE DISCIPLINE.—If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, such head shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

''(g) IMPROPER DISCLOSURE IS VIOLATION.—Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by this chapter is a violation of this chapter for purposes of this section.

''(h) CONSTRUCTION.—Nothing in this section may be construed to establish a new cause of action against any electronic communication service provider, remote computing service provider, geolocation service provider, or law enforcement or investigative officer, or eliminate or affect any cause of action that exists under section 2520, section 2707, or any other provision of law.''.

(b) CLERICAL AMENDMENT.—The table of chapters for part 1 of title 18, United States Code, is amended by inserting after the item relating to chapter 119 the following:

''120. Geolocation information ..... 2601''.

(c) CONFORMING AMENDMENTS.—Section 3512(a) of title 18, United States Code, is amended—

(1) in paragraph (2)—

(A) by redesignating subparagraphs (B), (C), and (D) as subparagraphs (C), (D), and (E), respectively; and

(B) by inserting after subparagraph (A) the following:

''(B) a warrant or order for geolocation information or records related thereto, as provided under section 2602 of this title;''.

SEC. 803. REQUIREMENT FOR SEARCH WARRANTS TO ACQUIRE GEOLOCATION INFORMATION.

Rule 41(a) of the Federal Rules of Criminal Procedure is amended—

(1) in paragraph (2)(A), by striking the period at the end and inserting a comma and ''including geolocation information.''; and

(2) by adding at the end the following:

''(F) 'Geolocation information' has the meaning given that term in section 2601 of title 18, United States Code.''.

SEC. 804. FRAUD AND RELATED ACTIVITY IN CONNECTION WITH OBTAINING GEOLOCATION INFORMATION.

(a) CRIMINAL VIOLATION.—Section 1039(h) of title 18, United States Code, is amended—

(1) in paragraph (2)—

(A) in subparagraph (A), by striking ''and'' at the end;

(B) in subparagraph (B), by striking the period at the end and inserting a semicolon and ''and''; and

(C) by adding at the end the following new subparagraph:

''(C) includes any geolocation information service.'';

(2) by redesignating paragraph (4) as paragraph (5); and

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

''(4) GEOLOCATION INFORMATION SERVICE.—The term 'geolocation information service' has the meaning given that term in section 2601.''.

(b) CONFORMING AMENDMENTS.—

(1) DEFINITION AMENDMENTS.—Section 1039(h)(1) of title 18, United States Code, is amended—

(A) in the paragraph heading, by inserting ''OR GPS'' after ''PHONE''; and

(B) in the matter preceding subparagraph (A), by inserting ''or GPS'' after ''phone''.

(2) CONFORMING AMENDMENTS.—Section 1039 of title 18, United States Code, is amended—

(A) in the section heading by inserting ''**or GPS**'' after ''**phone**'';

(B) in subsection (a)—

(i) in the matter preceding paragraph (1), by inserting ''or GPS'' after ''phone''; and

(ii) in paragraph (4), by inserting ''or GPS'' after ''phone'';

(C) in subsection (b)—

(i) in the subsection heading, by inserting ''OR GPS'' after ''PHONE'';

(ii) in paragraph (1), by inserting ''or GPS'' after ''phone'' both places that term appears; and

(iii) in paragraph (2), by inserting ''or GPS'' after ''phone''; and

(D) in subsection (c)—

(i) in the subsection heading, by inserting ''OR GPS'' after ''PHONE'';

(ii) in paragraph (1), by inserting ''or GPS'' after ''phone'' both places that term appears; and

(iii) in paragraph (2), by inserting ''or GPS'' after ''phone''.

(3) CHAPTER ANALYSIS.—The table of sections for chapter 47 of title 18, United States Code, is amended by striking the item relating to section 1039 and inserting the following:

''1039. Fraud and related activity in connection with obtaining confidential phone or GPS records information of a covered entity.''.

(c) SENTENCING GUIDELINES.—

(1) REVIEW AND AMENDMENT.—Not later than 180 days after the date of enactment of this Act, the United States Sentencing Commission, pursuant to its authority under section 994 of title 28, United States Code, and in accordance with this section, shall review and, if appropriate, amend the Federal sentencing guidelines and policy statements applicable to persons convicted of any offense under section 1039 of title 18, United States Code, as amended by this section.

(2) AUTHORIZATION.—The United States Sentencing Commission may amend the Federal sentencing guidelines in accordance with the procedures set forth in section 21(a) of the Sentencing Act of 1987 (28 U.S.C. 994 note) as though the authority under that section had not expired.

SEC. 805. STATEMENT OF EXCLUSIVE MEANS OF ACQUIRING GEOLOCATION INFORMATION.

(a) IN GENERAL.—No person may acquire the geolocation information of a person for protective activities or law enforcement or intelligence purposes except pursuant to a warrant issued pursuant to rule 41 of the Federal Rules of Criminal Procedure, as amended by section 803, or the amendments made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(b) GEOLOCATION INFORMATION DEFINED.—In this section, the term ''geolocation information'' has the meaning given that term in section 2601 of title 18, United States Code, as amended by section 802.

SA 2689. Mr. BENNET (for himself and Mr. COBURN) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE VIII—FEDERAL DATA CENTER CONSOLIDATION INITIATIVE

SEC. 801. DEFINITIONS.

In this title:

(1) ADMINISTRATOR.—The term ''Administrator'' means the Administrator for the Office of E-Government and Information Technology within the Office of Management and Budget.

(2) CHIEF INFORMATION OFFICERS COUNCIL.—The term ''Chief Information Officers Council'' means the Chief Information Officers Council established under section 3603 of title 44, United States Code.

(3) DATA CENTER.—

(A) DEFINITION.—The term ''data center'' means a closet, room, floor, or building for the storage, management, and dissemination of data and information, as defined by the Administrator in the ''Implementation Guidance for the Federal Data Center Consolidation Initiative'' memorandum, issued on March 19, 2012.

(B) AUTHORITY TO MODIFY DEFINITION.—The Administrator may promulgate guidance or other clarifications to modify the definition in subparagraph (A) in a manner consistent with this Act, as the Administrator determines necessary.

SEC. 802. FEDERAL DATA CENTER CONSOLIDATION INVENTORIES AND PLANS.

(a) REQUIRED SUBMISSIONS.—

(1) IN GENERAL.—

(A) ANNUAL REPORTS.—Each year, beginning in fiscal year 2013 through the end of fiscal year 2017, the head of each agency that is described in paragraph (2), assisted by the chief information officer of the agency, shall submit to the Administrator—

(i) by June 30th of each year, a comprehensive asset inventory of the data centers owned, operated, or maintained by or on behalf of the agency, even if the center is administered by a third party; and

(ii) by September 30th of each year, an updated consolidation plan that includes—

(I) a technical roadmap and approach for achieving the agency's targets for infrastructure utilization, energy efficiency, cost savings and efficiency;

(II) a detailed timeline for implementation of the data center consolidation plan;

(III) quantitative utilization and efficiency goals for reducing assets and improving use of information technology infrastructure;

(IV) performance metrics by which the progress of the agency toward data center consolidation goals can be measured, including metrics to track any gains in energy utilization as a result of this initiative;

(V) an aggregation of year-by-year investment and cost savings calculations for 5 years past the date of submission of the cost saving assessment, including a description of any initial costs for data center consolidation;

(VI) quantitative progress towards previously stated goals including cost savings and increases in operational efficiencies and utilization; and

(VII) any additional information required by the Administrator.

(B) CERTIFICATION.—Each year, beginning in fiscal year 2013 through the end of fiscal year 2017, the head of an agency, acting through the chief information officer of the agency, shall submit a statement to the Administrator certifying that the agency has complied with the requirements of this section.

(C) INSPECTOR GENERAL REPORT.—

(i) IN GENERAL.—The Inspector General for each agency described in paragraph (2) shall release a public report not later than 6 months after the date on which the agency releases the first updated asset inventory in fiscal year 2013 under subparagraph (A)(i), which shall evaluate the completeness of the inventory of the agency; and

(ii) AGENCY RESPONSE.—The head of each agency shall respond to the report completed by the Inspector General for the agency under clause (i), and complete any inventory identified by the Inspector General for the agency as incomplete, by the time the agency submits the required inventory update for fiscal year 2014.

(D) RESPONSIBILITY OF THE ADMINISTRATOR.—The Administrator shall ensure that each certification submitted under subparagraph (B) and each agency consolidation plan submitted under subparagraph (A)(ii), is made available in a timely fashion to the general public.

(2) AGENCIES DESCRIBED.—The agencies (including all associated components of the agency) described in this paragraph are the—

(A) Department of Agriculture;

(B) Department of Commerce;

(C) Department of Defense;

(D) Department of Education;

(E) Department of Energy;

(F) Department of Health and Human Services;

(G) Department of Homeland Security;

(H) Department of Housing and Urban Development;

(I) Department of the Interior;

(J) Department of Justice;

(K) Department of Labor;

(L) Department of State;

(M) Department of Transportation;

(N) Department of Treasury;

(O) Department of Veterans Affairs;

(P) Environmental Protection Agency;

(Q) General Services Administration;

(R) National Aeronautics and Space Administration;

(S) National Science Foundation;

(T) Nuclear Regulatory Commission;

(U) Office of Personnel Management;

(V) Small Business Administration;

(W) Social Security Administration; and

(X) United States Agency for International Development.

(3) AGENCY IMPLEMENTATION OF CONSOLIDATION PLANS.—Each agency described in paragraph (2), under the direction of the chief information officer of the agency, shall—

(A) implement the consolidation plan required under paragraph (1)(A)(ii); and

(B) provide to the Administrator annual updates on implementation and cost savings realized through such consolidation plan.

(b) ADMINISTRATOR REVIEW.—The Administrator shall—

(1) review the plans submitted under subsection (a) to determine whether each plan is comprehensive and complete;

(2) monitor the implementation of the data center consolidation plan of each agency described in subsection (a)(2); and

(3) update the cumulative cost savings projection on an annual basis as the savings are realized through the implementation of the agency plans.

(c) COST SAVING GOAL AND UPDATES FOR CONGRESS.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, or by September 30th of fiscal year 2013, whichever is later, the Administrator shall develop and publish a goal for the total amount of planned cost savings by the Federal Government through the Federal Data Center Consolidation Initiative during the 5-year period beginning on the date of enactment of this Act, which shall include a breakdown on a year-by-year basis of the projected savings.

(2) ANNUAL UPDATE.—

(A) IN GENERAL.—Not later than 1 year after the date on which the goal described in paragraph (1) is determined and each year thereafter until the end of 2017, the Administrator shall publish a report on the actual savings achieved through the Federal Data Center Consolidation Initiative as compared to the projected savings developed under paragraph (1) (based on data collected from each affected agency under subsection (a)(1)).

(B) UPDATE FOR CONGRESS.—The report required under subparagraph (A) shall be submitted to Congress and shall include an update on the progress made by each agency described in subsection (a)(2) on—

(i) whether each agency has in fact submitted a comprehensive asset inventory;

(ii) whether each agency has submitted a comprehensive consolidation plan with the key elements described in (a)(1)(A)(ii); and

(iii) the progress, if any, of each agency on implementing the consolidation plan of the agency.

(d) GAO REVIEW.—The Comptroller General of the United States shall, on an annual basis, publish a report on—

(1) the quality and completeness of each agency's asset inventory and consolidation plans required under subsection (a)(1)(A);

(2) each agency's progress on implementation of the consolidation plans submitted under subsection (a)(1)(A);

(3) overall planned and actual cost savings realized through implementation of the consolidation plans submitted under subsection (a)(1)(A);

(4) any steps that the Administrator could take to improve implementation of the data center consolidation initiative; and

(5) any matters for Congressional consideration in order to improve or accelerate the implementation of the data center consolidation initiative.

(e) RESPONSE TO GAO.—

(1) IN GENERAL.—If a report required under subsection (d) identifies any deficiencies or delays in any of the elements described in paragraphs (1) through (5) of subsection (d) for an agency, the head of the agency shall respond in writing to the Comptroller General of the United State, not later than 90 days after the date on which the report is published under subsection (d), with a detailed explanation of how the agency will address the deficiency.

(2) ADDITIONAL REQUIREMENTS.—If the Comptroller General identifies an agency that has repeatedly lagged in implementing the data center consolidation initiative, the Comptroller General may require that the head of the agency submit a statement explaining—

(A) why the agency is having difficulty implementing the initiative; and

(B) what structural or personnel changes are needed within the agency to address the problem.

SEC. 803. ENSURING CYBERSECURITY STANDARDS FOR DATA CENTER CONSOLIDATION AND CLOUD COMPUTING.

An agency required to implement a data center consolidation plan under this title and migrate to cloud computing shall do so in a manner that is consistent with Federal guidelines on cloud computing security, including—

(1) applicable provisions found within the Federal Risk and Authorization Management Program of the General Service Administration; and

(2) guidance published by the National Institute of Standards and Technology.

SEC. 804. CLASSIFIED INFORMATION.

The Director of National Intelligence may waive the requirements of this title for any element (or component of an element) of the intelligence community.

SEC. 805. SUNSET.

This title is repealed effective on October 1, 2017.

SA 2690. Ms. MURKOWSKI submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of section 104, add the following:

(d) APPLICATION OF BENEFITS OF CYBERSECURITY PROGRAM TO ENTITIES SUBJECT TO MANDATORY REQUIREMENTS.—

(1) IN GENERAL.—Subject to paragraphs (2) through (4), any entity subject to the jurisdiction of the Federal Energy Regulatory Commission under section 215 of the Federal Power Act (16 U.S.C. 824o) or to any facility subject to cybersecurity measures required by the Nuclear Regulatory Commission under the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.) shall be entitled to the benefits of certification provided under subsection (c) (other than subsection (c)(1)).

(2) ELIGIBILITY.—To be eligible for the benefits of certification described in paragraph (1), an entity or facility shall demonstrate to the Secretary of Energy that it is an entity or facility described in paragraph (1).

(3) CERTIFIED OWNER OR OPERATOR.—If the Secretary of Energy determines that an entity or facility is an entity or facility described in paragraph (1), the entity or facility shall be considered a certified owner or operator under this section (other than subsection (c)(1)).

(4) EFFECT ON OTHER LAWS.—Nothing in this subsection limits the applicability of any exemption from or limitation of liability or damages that a certified owner may have under any other Federal or State law (including regulations).

(e) FEDERAL ENERGY LAWS.—Except as provided in subsection (d), nothing in this Act authorizes the imposition or modification of requirements relating to—

(1)(A) the bulk-power system;

(B) the promulgation or enforcement of reliability standards for the bulk power system (including for cybersecurity protection) by the certified Electric Reliability Organization; or

(C) the approval or enforcement of the standards by the Federal Energy Regulatory Commission under section 215 of the Federal Power Act (16 U.S.C. 824o); or

(2) nuclear facilities subject to cybersecurity measures required by the Nuclear Regulatory Commission under the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.).

SA 2691. Mrs. HUTCHISON submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Strike title I.

SA 2692. Mrs. HUTCHISON (for herself, Mr. MCCAIN, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 1, strike line 4 and all that follows and insert the following:

(a) SHORT TITLE.—This Act may be cited as the ''Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012'' or ''SECURE IT''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

TITLE I—FACILITATING SHARING OF CYBER THREAT INFORMATION

SEC. 101. DEFINITIONS.

In this title:

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

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

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

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

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

(3) COUNTERMEASURE.—The term ''countermeasure'' means an automated or a manual action with defensive intent to mitigate cyber threats.

(4) CYBER THREAT INFORMATION.—The term ''cyber threat information'' means information that indicates or describes—

(A) a technical or operation vulnerability or a cyber threat mitigation measure;

(B) an action or operation to mitigate a cyber threat;

(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

(D) a method of defeating a technical control;

(E) a method of defeating an operational control;

(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

(G) 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 inadvertently enable the defeat of a technical or operational control;

(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

(J) any combination of subparagraphs (A) through (I).

(5) CYBERSECURITY CENTER.—The term ''cybersecurity center'' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

(6) CYBERSECURITY SYSTEM.—The term ''cybersecurity system'' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or to safeguard, a system or network, including measures intended to protect a system or network from—

(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriations of private or government information, intellectual property, or personally identifiable information.

(7) ENTITY.—

(A) IN GENERAL.—The term ''entity'' means any private entity, non-Federal government agency or department, or State, tribal, or local government agency or department (including an officer, employee, or agent thereof).

(B) INCLUSIONS.—The term ''entity'' includes a government agency or department (including an officer, employee, or agent thereof) 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.

(8) FEDERAL INFORMATION SYSTEM.—The term ''Federal information system'' means an information system of a Federal department or agency used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

(9) INFORMATION SECURITY.—The term ''information security'' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

(C) availability, by ensuring timely and reliable access to and use of information.

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

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

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

(13) OPERATIONAL CONTROL.—The term ''operational control'' means a security control for an information system that primarily is implemented and executed by people.

(14) OPERATIONAL VULNERABILITY.—The term ''operational vulnerability'' means any attribute of policy, process, or procedure that could enable or facilitate the defeat of an operational control.

(15) PRIVATE ENTITY.—The term ''private entity'' means any individual or any private group, organization, or corporation, including an officer, employee, or agent thereof.

(16) SIGNIFICANT CYBER INCIDENT.—The term ''significant cyber incident'' means a cyber incident resulting in, or an attempted

cyber incident that, if successful, would have resulted in—

(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

(17) TECHNICAL CONTROL.—The term ''technical control'' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

(18) TECHNICAL VULNERABILITY.—The term ''technical vulnerability'' means any attribute of hardware or software that could enable or facilitate the defeat of a technical control.

(19) 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. 102. AUTHORIZATION TO SHARE CYBER THREAT INFORMATION.

(a) VOLUNTARY DISCLOSURE.—

(1) PRIVATE ENTITIES.—Notwithstanding any other provision of law, a private entity may, for the purpose of preventing, investigating, or otherwise mitigating threats to information security, on its own networks, or as authorized by another entity, on such entity's networks, employ countermeasures and use cybersecurity systems in order to obtain, identify, or otherwise possess cyber threat information.

(2) ENTITIES.—Notwithstanding any other provision of law, an entity may disclose cyber threat information to—

(A) a cybersecurity center; or

(B) any other entity in order to assist with preventing, investigating, or otherwise mitigating threats to information security.

(3) INFORMATION SECURITY PROVIDERS.—If the cyber threat information described in paragraph (1) is obtained, identified, or otherwise possessed in the course of providing information security products or services under contract to another entity, that entity shall be given, at any time prior to disclosure of such information, a reasonable opportunity to authorize or prevent such disclosure, to request anonymization of such information, or to request that reasonable efforts be made to safeguard such information that identifies specific persons from unauthorized access or disclosure.

(b) SIGNIFICANT CYBER INCIDENTS INVOLVING FEDERAL INFORMATION SYSTEMS.—

(1) IN GENERAL.—An entity providing electronic communication services, remote computing services, or information security services to a Federal department or agency shall inform the Federal department or agency of a significant cyber incident involving the Federal information system of that Federal department or agency that—

(A) is directly known to the entity as a result of providing such services;

(B) is directly related to the provision of such services by the entity; and

(C) as determined by the entity, has impeded or will impede the performance of a critical mission of the Federal department or agency.

(2) ADVANCE COORDINATION.—A Federal department or agency receiving the services described in paragraph (1) shall coordinate in advance with an entity described in paragraph (1) to develop the parameters of any information that may be provided under paragraph (1), including clarification of the type of significant cyber incident that will impede the performance of a critical mission of the Federal department or agency.

(3) REPORT.—A Federal department or agency shall report information provided under this subsection to a cybersecurity center.

(4) CONSTRUCTION.—Any information provided to a cybersecurity center under paragraph (3) shall be treated in the same manner as information provided to a cybersecurity center under subsection (a).

(c) INFORMATION SHARED WITH OR PROVIDED TO A CYBERSECURITY CENTER.—Cyber threat information provided to a cybersecurity center under this section—

(1) may be disclosed to, retained by, and used by, consistent with otherwise applicable Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal government for a cybersecurity purpose, a national security purpose, or in order to prevent, investigate, or prosecute any of the offenses listed in section 2516 of title 18, United States Code, and such information shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under this paragraph;

(2) may, with the prior written consent of the entity submitting such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(3) shall be considered the commercial, financial, or proprietary information of the entity providing such information to the Federal government and any disclosure outside the Federal government may only be made upon the prior written consent by such entity and shall not constitute a waiver of any applicable privilege or protection provided by law, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(4) shall be 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;

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

(6) shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official;

(7) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to any entity by such State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent; and

(8) shall not be directly used by any Federal, State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph.

(d) PROCEDURES RELATING TO INFORMATION SHARING WITH A CYBERSECURITY CENTER.—Not later than 60 days after the date of enactment of this Act, the heads of each department or agency containing a cybersecurity center shall jointly develop, promulgate, and submit to Congress procedures to ensure that cyber threat information shared with or provided to—

(1) a cybersecurity center under this section—

(A) may be submitted to a cybersecurity center by an entity, to the greatest extent possible, through a uniform, publicly available process or format that is easily accessible on the website of such cybersecurity center, and that includes the ability to provide relevant details about the cyber threat information and written consent to any subsequent disclosures authorized by this paragraph;

(B) shall immediately be further shared with each cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government;

(C) is handled by the Federal government in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title, and the Federal government may undertake efforts consistent with this subparagraph to limit the impact on privacy and civil liberties of the sharing of cyber threat information with the Federal government; and

(D) except as provided in this section, shall only be used, disclosed, or handled in accordance with the provisions of subsection (c); and

(2) a Federal agency or department under subsection (b) is provided immediately to a cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government.

(e) INFORMATION SHARED BETWEEN ENTITIES.—

(1) IN GENERAL.—An entity sharing cyber threat information with another entity under this title may restrict the use or sharing of such information by such other entity.

(2) FURTHER SHARING.—Cyber threat information shared by any entity with another entity under this title—

(A) shall only be further shared in accordance with any restrictions placed on the sharing of such information by the entity authorizing such sharing, such as appropriate anonymization of such information; and

(B) may not be used by any entity to gain an unfair competitive advantage to the detriment of the entity authorizing the sharing of such information, except that the conduct described in paragraph (3) shall not constitute unfair competitive conduct.

(3) INFORMATION SHARED WITH STATE, TRIBAL, OR LOCAL GOVERNMENT OR GOVERNMENT AGENCY.—Cyber threat information shared with a State, tribal, or local government or government agency under this title—

(A) may, with the prior written consent of the entity sharing such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent;

(B) shall be deemed voluntarily shared information and exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records;

(C) shall not be disclosed or distributed to any entity by the State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent; and

(D) shall not be directly used by any State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this subparagraph.

(4) ANTITRUST EXEMPTION.—The exchange or provision of cyber threat information or assistance between 2 or more private entities under this title shall not be considered a violation of any provision of antitrust laws if exchanged or provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of threats to information security; or

(B) communicating or disclosing of cyber threat information to help prevent, investigate or otherwise mitigate the effects of a threat to information security.

(5) NO RIGHT OR BENEFIT.—The provision of cyber threat information to an entity under this section shall not create a right or a benefit to similar information by such entity or any other entity.

(f) FEDERAL PREEMPTION.—

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

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

(3) PUBLIC DISCLOSURE.—No information shared with or provided to a State, tribal, or local government or government agency pursuant to this section shall be made publicly available pursuant to any State, tribal, or local law requiring disclosure of information or records.

(g) CIVIL AND CRIMINAL LIABILITY.—

(1) GENERAL PROTECTIONS.—

(A) PRIVATE ENTITIES.—No cause of action shall lie or be maintained in any court against any private entity for—

(i) the use of countermeasures and cybersecurity systems as authorized by this title;

(ii) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(iii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such private entity.

(B) ENTITIES.—No cause of action shall lie or be maintained in any court against any entity for—

(i) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(ii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such entity.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed 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, and use of classified information.

(h) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this section shall be construed to limit or prohibit otherwise lawful disclosures of communications, records, or other information by a private entity to any other governmental or private entity not covered under this section.

(i) WHISTLEBLOWER PROTECTION.—Nothing in this Act shall be construed to preempt or preclude any employee from exercising rights currently provided under any whistleblower law, rule, or regulation.

(j) RELATIONSHIP TO OTHER LAWS.—The submission of cyber threat information under this section to a cybersecurity center shall not affect any requirement under any other provision of law for an entity to provide information to the Federal government.

SEC. 103. INFORMATION SHARING BY THE FEDERAL GOVERNMENT.

(a) CLASSIFIED INFORMATION.—

(1) PROCEDURES.—Consistent with the protection of intelligence sources and methods, and as otherwise determined appropriate, the Director of National Intelligence and the Secretary of Defense, in consultation with the heads of the appropriate Federal departments or agencies, shall develop and promulgate procedures to facilitate and promote—

(A) the immediate sharing, through the cybersecurity centers, of classified cyber threat information in the possession of the Federal government with appropriately cleared representatives of any appropriate entity; and

(B) the declassification and immediate sharing, through the cybersecurity centers, with any entity or, if appropriate, public availability of cyber threat information in the possession of the Federal government;

(2) HANDLING OF CLASSIFIED INFORMATION.—The procedures developed under paragraph (1) shall ensure that each entity receiving classified cyber threat information pursuant to this section has acknowledged in writing the ongoing obligation to comply with all laws, executive orders, and procedures concerning the appropriate handling, disclosure, or use of classified information.

(b) UNCLASSIFIED CYBER THREAT INFORMATION.—The heads of each department or agency containing a cybersecurity center shall jointly develop and promulgate procedures that ensure that, consistent with the provisions of this section, unclassified, including controlled unclassified, cyber threat information in the possession of the Federal government—

(1) is shared, through the cybersecurity centers, in an immediate and adequate manner with appropriate entities; and

(2) if appropriate, is made publicly available.

(c) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed under this section shall incorporate, to the greatest extent possible, existing processes utilized by sector specific information sharing and analysis centers.

(2) COORDINATION WITH ENTITIES.—In developing the procedures required under this section, the Director of National Intelligence and the heads of each department or agency containing a cybersecurity center shall coordinate with appropriate entities to ensure that protocols are implemented that will facilitate and promote the sharing of cyber threat information by the Federal government.

(d) ADDITIONAL RESPONSIBILITIES OF CYBERSECURITY CENTERS.—Consistent with section 102, a cybersecurity center shall—

(1) facilitate information sharing, interaction, and collaboration among and between cybersecurity centers and—

(A) other Federal entities;

(B) any entity; and

(C) international partners, in consultation with the Secretary of State;

(2) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of information systems; and

(3) coordinate with other Federal entities, as appropriate, to integrate information from across the Federal government to provide situational awareness of the cybersecurity posture of the United States.

(e) SHARING WITHIN THE FEDERAL GOVERNMENT.—The heads of appropriate Federal departments and agencies shall ensure that cyber threat information in the possession of such Federal departments or agencies that relates to the prevention, investigation, or mitigation of threats to information security across the Federal government is shared effectively with the cybersecurity centers.

(f) SUBMISSION TO CONGRESS.—Not later than 60 days after the date of enactment of this Act, the Director of National Intelligence, in coordination with the appropriate head of a department or an agency containing a cybersecurity center, shall submit the procedures required by this section to Congress.

SEC. 104. CONSTRUCTION.

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

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

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any entity and the Federal government, except as specified under section 102(b); or

(4) to modify the authority of a department or agency of the Federal government to protect sources and methods and the national security of the United States.

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

(1) to require an entity to share information with the Federal government, except as expressly provided under section 102(b); or

(2) to condition the sharing of cyber threat information with an entity on such entity's provision of cyber threat information to the Federal government.

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

(d) USE AND RETENTION OF INFORMATION.—Nothing in this title shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal government to retain or use any information shared under section 102 for any use other than a use permitted under section 102(c)(1).

(e) NO NEW FUNDING.—An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 105. REPORT ON IMPLEMENTATION.

(a) CONTENT OF REPORT.—Not later than 1 year after the date of enactment of this Act, and biennially thereafter, the heads of each department or agency containing a cybersecurity center shall jointly submit, in coordination with the privacy and civil liberties officials of such departments or agencies and the Privacy and Civil Liberties Oversight

Board, a detailed report to Congress concerning the implementation of this title, including—

(1) an assessment of the sufficiency of the procedures developed under section 103 of this Act in ensuring that cyber threat information in the possession of the Federal government is provided in an immediate and adequate manner to appropriate entities or, if appropriate, is made publicly available;

(2) an assessment of whether information has been appropriately classified and an accounting of the number of security clearances authorized by the Federal government for purposes of this title;

(3) a review of the type of cyber threat information shared with a cybersecurity center under section 102 of this Act, including whether such information meets the definition of cyber threat information under section 101, the degree to which such information may impact the privacy and civil liberties of individuals, any appropriate metrics to determine any impact of the sharing of such information with the Federal government on privacy and civil liberties, and the adequacy of any steps taken to reduce such impact;

(4) a review of actions taken by the Federal government based on information provided to a cybersecurity center under section 102 of this Act, including the appropriateness of any subsequent use under section 102(c)(1) of this Act and whether there was inappropriate stovepiping within the Federal government of any such information;

(5) a description of any violations of the requirements of this title by the Federal government;

(6) a classified list of entities that received classified information from the Federal government under section 103 of this Act and a description of any indication that such information may not have been appropriately handled;

(7) a summary of any breach of information security, if known, attributable to a specific failure by any entity or the Federal government to act on cyber threat information in the possession of such entity or the Federal government that resulted in substantial economic harm or injury to a specific entity or the Federal government; and

(8) any recommendation for improvements or modifications to the authorities under this title.

(b) FORM OF REPORT.—The report under subsection (a) shall be submitted in unclassified form, but shall include a classified annex.

SEC. 106. INSPECTOR GENERAL REVIEW.

(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency are authorized to review compliance by the cybersecurity centers, and by any Federal department or agency receiving cyber threat information from such cybersecurity centers, with the procedures required under section 102 of this Act.

(b) SCOPE OF REVIEW.—The review under subsection (a) shall consider whether the Federal government has handled such cyber threat information in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title.

(c) REPORT TO CONGRESS.—Each review conducted under this section shall be provided to Congress not later than 30 days after the date of completion of the review.

SEC. 107. TECHNICAL AMENDMENTS.

Section 552(b) of title 5, United States Code, is amended—

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

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

(3) by adding at the end the following:

''(10) information shared with or provided to a cybersecurity center under section 102 of title I of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012.''.

SEC. 108. ACCESS TO CLASSIFIED INFORMATION.

(a) AUTHORIZATION REQUIRED.—No person shall be provided with access to classified information (as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 435 note; relating to classified national security information)) relating to cyber security threats or cyber security vulnerabilities under this title without the appropriate security clearances.

(b) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall, consistent with applicable procedures and requirements, and if otherwise deemed appropriate, assist an individual in timely obtaining an appropriate security clearance where such individual has been determined to be eligible for such clearance and has a need-to-know (as defined in section 6.1 of that Executive Order) classified information to carry out this title.

TITLE II—COORDINATION OF FEDERAL INFORMATION SECURITY POLICY

SEC. 201. COORDINATION OF FEDERAL INFORMATION SECURITY POLICY.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3551. Purposes

''The purposes of this subchapter are—

''(1) to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

''(2) to recognize the highly networked nature of the current Federal computing environment and provide effective government-wide management of policies, directives, standards, and guidelines, as well as effective and nimble oversight of and response to information security risks, including coordination of information security efforts throughout the Federal civilian, national security, and law enforcement communities;

''(3) to provide for development and maintenance of controls required to protect agency information and information systems and contribute to the overall improvement of agency information security posture;

''(4) to provide for the development of tools and methods to assess and respond to real-time situational risk for Federal information system operations and assets; and

''(5) to provide a mechanism for improving agency information security programs through continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

''§ 3552. Definitions

''In this subchapter:

''(1) ADEQUATE SECURITY.—The term 'adequate security' means security commensurate with the risk and magnitude of the harm resulting from the unauthorized access to or loss, misuse, destruction, or modification of information.

''(2) AGENCY.—The term 'agency' has the meaning given the term in section 3502 of title 44.

''(3) CYBERSECURITY CENTER.—The term 'cybersecurity center' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

''(4) CYBER THREAT INFORMATION.—The term 'cyber threat information' means information that indicates or describes—

''(A) a technical or operation vulnerability or a cyber threat mitigation measure;

''(B) an action or operation to mitigate a cyber threat;

''(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

''(D) a method of defeating a technical control;

''(E) a method of defeating an operational control;

''(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

''(G) 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 inadvertently enable the defeat of a technical or operational control;

''(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

''(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

''(J) any combination of subparagraphs (A) through (I).

''(5) DIRECTOR.—The term 'Director' means the Director of the Office of Management and Budget unless otherwise specified.

''(6) ENVIRONMENT OF OPERATION.—The term 'environment of operation' means the information system and environment in which those systems operate, including changing threats, vulnerabilities, technologies, and missions and business practices.

''(7) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

''(8) INCIDENT.—The term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

''(B) constitutes a violation of law or an imminent threat of violation of a law, a security policy, a security procedure, or an acceptable use policy.

''(9) INFORMATION RESOURCES.—The term 'information resources' has the meaning given the term in section 3502 of title 44.

''(10) INFORMATION SECURITY.—The term 'information security' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

''(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

''(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

''(C) availability, by ensuring timely and reliable access to and use of information.

''(11) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44.

''(12) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 11101 of title 40.

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

''(14) NATIONAL SECURITY SYSTEM.—

''(A) IN GENERAL.—The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(B) LIMITATION.—Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

''(15) OPERATIONAL CONTROL.—The term 'operational control' means a security control for an information system that primarily is implemented and executed by people.

''(16) PERSON.—The term 'person' has the meaning given the term in section 3502 of title 44.

''(17) SECRETARY.—The term 'Secretary' means the Secretary of Commerce unless otherwise specified.

''(18) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls, including safeguards or countermeasures, prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

''(19) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

''(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

''(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

''(20) TECHNICAL CONTROL.—The term 'technical control' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

''§ 3553. Federal information security authority and coordination

''(a) IN GENERAL.—The Secretary, in consultation with the Secretary of Homeland Security, shall—

''(1) issue compulsory and binding policies and directives governing agency information security operations, and require implementation of such policies and directives, including—

''(A) policies and directives consistent with the standards and guidelines promulgated under section 11331 of title 40 to identify and provide information security protections prioritized and commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by or on behalf of an agency; or

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(B) minimum operational requirements for Federal Government to protect agency information systems and provide common situational awareness across all agency information systems;

''(C) reporting requirements, consistent with relevant law, regarding information security incidents and cyber threat information;

''(D) requirements for agencywide information security programs;

''(E) performance requirements and metrics for the security of agency information systems;

''(F) training requirements to ensure that agencies are able to fully and timely comply with the policies and directives issued by the Secretary under this subchapter;

''(G) training requirements regarding privacy, civil rights, and civil liberties, and information oversight for agency information security personnel;

''(H) requirements for the annual reports to the Secretary under section 3554(d);

''(I) any other information security operations or information security requirements as determined by the Secretary in coordination with relevant agency heads; and

''(J) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(2) review the agencywide information security programs under section 3554; and

''(3) designate an individual or an entity at each cybersecurity center, among other responsibilities—

''(A) to receive reports and information about information security incidents, cyber threat information, and deterioration of security control affecting agency information systems; and

''(B) to act on or share the information under subparagraph (A) in accordance with this subchapter.

''(b) CONSIDERATIONS.—When issuing policies and directives under subsection (a), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology under section 11331 of title 40.

''(c) LIMITATION OF AUTHORITY.—The authorities of the Secretary under this section shall not apply to national security systems. Information security policies, directives, standards and guidelines for national security systems shall be overseen as directed by the President and, in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

''(d) STATUTORY CONSTRUCTION.—Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any head of an agency over such agency.

''§ 3554. Agency responsibilities

''(a) IN GENERAL.—The head of each agency shall—

''(1) be responsible for—

''(A) complying with the policies and directives issued under section 3553;

''(B) providing information security protections commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by the agency or by a contractor of an agency or other organization on behalf of an agency; and

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(C) complying with the requirements of this subchapter, including—

''(i) information security standards and guidelines promulgated under section 11331 of title 40;

''(ii) for any national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued as directed by the President; and

''(iii) for any non-national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued under section 3553;

''(D) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

''(E) reporting and sharing, for an agency operating or exercising control of a national security system, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for national security systems issued as directed by the President; and

''(F) reporting and sharing, for those agencies operating or exercising control of non-national security systems, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for non-national security systems as prescribed under section 3553(a), including information to assist the entity designated under section 3555(a) with the ongoing security analysis under section 3555;

''(2) ensure that each senior agency official provides information security for the information and information systems that support the operations and assets under the senior agency official's control, including by—

''(A) assessing the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

''(B) determining the level of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3553(a), and standards and guidelines promulgated under section 11331 of title 40 for information security classifications and related requirements;

''(C) implementing policies, procedures, and capabilities to reduce risks to an acceptable level in a cost-effective manner;

''(D) actively monitoring the effective implementation of information security controls and techniques; and

''(E) reporting information about information security incidents, cyber threat information, and deterioration of security controls in a timely and adequate manner to the entity designated under section 3553(a)(3) in accordance with paragraph (1);

''(3) assess and maintain the resiliency of information technology systems critical to agency mission and operations;

''(4) designate the agency Inspector General (or an independent entity selected in consultation with the Director and the Council of Inspectors General on Integrity and Efficiency if the agency does not have an Inspector General) to conduct the annual independent evaluation required under section 3556, and allow the agency Inspector General to contract with an independent entity to perform such evaluation;

''(5) delegate to the Chief Information Officer or equivalent (or to a senior agency official who reports to the Chief Information Officer or equivalent)—

''(A) the authority and primary responsibility to implement an agencywide information security program; and

''(B) the authority to provide information security for the information collected and maintained by the agency (or by a contractor, other agency, or other source on behalf of the agency) and for the information systems that support the operations, assets, and mission of the agency (including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency);

''(6) delegate to the appropriate agency official (who is responsible for a particular agency system or subsystem) the responsibility to ensure and enforce compliance with all requirements of the agency's agencywide information security program in coordination with the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5);

''(7) ensure that an agency has trained personnel who have obtained any necessary security clearances to permit them to assist the agency in complying with this subchapter;

''(8) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5), in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agencywide information security program, including the progress of any remedial actions; and

''(9) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5) has the necessary qualifications to administer the functions described in this subchapter and has information security duties as a primary duty of that official.

''(b) CHIEF INFORMATION OFFICERS.—Each Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under subsection (a)(5) shall—

''(1) establish and maintain an enterprise security operations capability that on a continuous basis—

''(A) detects, reports, contains, mitigates, and responds to information security incidents that impair adequate security of the agency's information or information system in a timely manner and in accordance with the policies and directives under section 3553; and

''(B) reports any information security incident under subparagraph (A) to the entity designated under section 3555;

''(2) develop, maintain, and oversee an agencywide information security program;

''(3) develop, maintain, and oversee information security policies, procedures, and control techniques to address applicable requirements, including requirements under section 3553 of this title and section 11331 of title 40; and

''(4) train and oversee the agency personnel who have significant responsibility for information security with respect to that responsibility.

''(c) AGENCYWIDE INFORMATION SECURITY PROGRAMS.—

''(1) IN GENERAL.—Each agencywide information security program under subsection (b)(2) shall include—

''(A) relevant security risk assessments, including technical assessments and others related to the acquisition process;

''(B) security testing commensurate with risk and impact;

''(C) mitigation of deterioration of security controls commensurate with risk and impact;

''(D) risk-based continuous monitoring and threat assessment of the operational status and security of agency information systems to enable evaluation of the effectiveness of and compliance with information security policies, procedures, and practices, including a relevant and appropriate selection of security controls of information systems identified in the inventory under section 3505(c);

''(E) operation of appropriate technical capabilities in order to detect, mitigate, report, and respond to information security incidents, cyber threat information, and deterioration of security controls in a manner that is consistent with the policies and directives under section 3553, including—

''(i) mitigating risks associated with such information security incidents;

''(ii) notifying and consulting with the entity designated under section 3555; and

''(iii) notifying and consulting with, as appropriate—

''(I) law enforcement and the relevant Office of the Inspector General; and

''(II) any other entity, in accordance with law and as directed by the President;

''(F) a process to ensure that remedial action is taken to address any deficiencies in the information security policies, procedures, and practices of the agency; and

''(G) a plan and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency.

''(2) RISK MANAGEMENT STRATEGIES.—Each agencywide information security program under subsection (b)(2) shall include the development and maintenance of a risk management strategy for information security. The risk management strategy shall include—

''(A) consideration of information security incidents, cyber threat information, and deterioration of security controls; and

''(B) consideration of the consequences that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency;

''(3) POLICIES AND PROCEDURES.—Each agencywide information security program under subsection (b)(2) shall include policies and procedures that—

''(A) are based on the risk management strategy under paragraph (2);

''(B) reduce information security risks to an acceptable level in a cost-effective manner;

''(C) ensure that cost-effective and adequate information security is addressed as part of the acquisition and ongoing management of each agency information system; and

''(D) ensure compliance with—

''(i) this subchapter; and

''(ii) any other applicable requirements.

''(4) TRAINING REQUIREMENTS.—Each agencywide information security program under subsection (b)(2) shall include information security, privacy, civil rights, civil liberties, and information oversight training that meets any applicable requirements under section 3553. The training shall inform each information security personnel that has access to agency information systems (including contractors and other users of information systems that support the operations and assets of the agency) of—

''(A) the information security risks associated with the information security personnel's activities; and

''(B) the individual's responsibility to comply with the agency policies and procedures that reduce the risks under subparagraph (A).

''(d) ANNUAL REPORT.—Each agency shall submit a report annually to the Secretary of Homeland Security on its agencywide information security program and information systems.

''§ 3555. Multiagency ongoing threat assessment

''(a) IMPLEMENTATION.—The Director of the Office of Management and Budget, in coordination with the Secretary of Homeland Security, shall designate an entity to implement ongoing security analysis concerning agency information systems—

''(1) based on cyber threat information;

''(2) based on agency information system and environment of operation changes, including—

''(A) an ongoing evaluation of the information system security controls; and

''(B) the security state, risk level, and environment of operation of an agency information system, including—

''(i) a change in risk level due to a new cyber threat;

''(ii) a change resulting from a new technology;

''(iii) a change resulting from the agency's mission; and

''(iv) a change resulting from the business practice; and

''(3) using automated processes to the maximum extent possible—

''(A) to increase information system security;

''(B) to reduce paper-based reporting requirements; and

''(C) to maintain timely and actionable knowledge of the state of the information system security.

''(b) STANDARDS.—The National Institute of Standards and Technology may promulgate standards, in coordination with the Secretary of Homeland Security, to assist an agency with its duties under this section.

''(c) COMPLIANCE.—The head of each appropriate department and agency shall be responsible for ensuring compliance and implementing necessary procedures to comply with this section. The head of each appropriate department and agency, in consultation with the Director of the Office of Management and Budget and the Secretary of Homeland Security, shall—

''(1) monitor compliance under this section;

''(2) develop a timeline and implement for the department or agency—

''(A) adoption of any technology, system, or method that facilitates continuous monitoring and threat assessments of an agency information system;

''(B) adoption or updating of any technology, system, or method that prevents, detects, or remediates a significant cyber incident to a Federal information system of the department or agency that has impeded, or is reasonably likely to impede, the performance of a critical mission of the department or agency; and

''(C) adoption of any technology, system, or method that satisfies a requirement under this section.

''(d) LIMITATION OF AUTHORITY.—The authorities of the Director of the Office of Management and Budget and of the Secretary of Homeland Security under this section shall not apply to national security systems.

''(e) REPORT.—Not later than 6 months after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Government Accountability Office shall issue a report evaluating each agency's status toward implementing this section.

''§ 3556. Independent evaluations

''(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency, in consultation with the Director and the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense, shall issue and maintain criteria for the timely, cost-effective, risk-based, and independent evaluation of each agencywide information security program (and practices) to determine the effectiveness of the agencywide information security program (and practices). The criteria shall include measures to assess any conflicts of interest in the performance of the evaluation and whether the agencywide information security program includes appropriate safeguards against disclosure of information where such disclosure may adversely affect information security.

''(b) ANNUAL INDEPENDENT EVALUATIONS.—Each agency shall perform an annual independent evaluation of its agencywide information security program (and practices) in accordance with the criteria under subsection (a).

''(c) DISTRIBUTION OF REPORTS.—Not later than 30 days after receiving an independent evaluation under subsection (b), each agency head shall transmit a copy of the independent evaluation to the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense.

''(d) NATIONAL SECURITY SYSTEMS.—Evaluations involving national security systems shall be conducted as directed by President.

''§ 3557. National security systems.

''The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

''(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system; and

''(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President.''.

(b) SAVINGS PROVISIONS.—

(1) POLICY AND COMPLIANCE GUIDANCE.—Policy and compliance guidance issued by the Director before the date of enactment of this Act under section 3543(a)(1) of title 44, United States Code (as in effect on the day before the date of enactment of this Act), shall continue in effect, according to its terms, until modified, terminated, superseded, or repealed pursuant to section 3553(a)(1) of title 44, United States Code.

(2) STANDARDS AND GUIDELINES.—Standards and guidelines issued by the Secretary of Commerce or by the Director before the date of enactment of this Act under section 11331(a)(1) of title 40, United States Code, (as in effect on the day before the date of enactment of this Act) shall continue in effect, according to their terms, until modified, terminated, superseded, or repealed pursuant to section 11331(a)(1) of title 40, United States Code, as amended by this Act.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) CHAPTER ANALYSIS.—The chapter analysis for chapter 35 of title 44, United States Code, is amended—

(A) by striking the items relating to sections 3531 through 3538;

(B) by striking the items relating to sections 3541 through 3549; and

(C) by inserting the following:

''3551. Purposes.
''3552. Definitions.
''3553. Federal information security authority and coordination.
''3554. Agency responsibilities.
''3555. Multiagency ongoing threat assessment.
''3556. Independent evaluations.
''3557. National security systems.''.

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3552''.

(B) Section 2222(j)(5) of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(C) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(D) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(E) Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3532(b)(2)'' and inserting ''section 3552'';

(ii) in subsection (c)(3), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iii) in subsection (d)(1), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iv) in subsection (d)(8) by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(v) in subsection (d)(8), by striking ''submitted to the Director'' and inserting ''submitted to the Secretary'';

(vi) in subsection (e)(2), by striking ''section 3532(1) of such title'' and inserting ''section 3552 of title 44''; and

(vii) in subsection (e)(5), by striking ''section 3532(b)(2) of such title'' and inserting ''section 3552 of title 44''.

(F) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking ''section 3534(b)'' and inserting ''section 3554(b)(2)''.

SEC. 202. MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) IN GENERAL.—Section 11331 of title 40, United States Code, is amended to read as follows:

''§ 11331. Responsibilities for Federal information systems standards

''(a) STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO PRESCRIBE.—Except as provided under paragraph (2), the Secretary of Commerce shall prescribe standards and guidelines pertaining to Federal information systems—

''(A) in consultation with the Secretary of Homeland Security; and

''(B) on the basis of standards and guidelines developed by the National Institute of Standards and Technology under paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)(2) and (a)(3)).

''(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.

''(b) MANDATORY STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO MAKE MANDATORY STANDARDS AND GUIDELINES.—The Secretary of Commerce shall make standards and guidelines under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of Federal information systems.

''(2) REQUIRED MANDATORY STANDARDS AND GUIDELINES.—

''(A) IN GENERAL.—Standards and guidelines under subsection (a)(1) shall include information security standards that—

''(i) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

''(ii) are otherwise necessary to improve the security of Federal information and information systems.

''(B) BINDING EFFECT.—Information security standards under subparagraph (A) shall be compulsory and binding.

''(c) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary of Commerce shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director.

''(d) APPLICATION OF MORE STRINGENT STANDARDS AND GUIDELINES.—The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards and guidelines the Secretary of Commerce prescribes under this section if the more stringent standards and guidelines—

''(1) contain at least the applicable standards and guidelines made compulsory and binding by the Secretary of Commerce; and

''(2) are otherwise consistent with the policies, directives, and implementation memoranda issued under section 3553(a) of title 44.

''(e) DECISIONS ON PROMULGATION OF STANDARDS AND GUIDELINES.—The decision by the Secretary of Commerce regarding the promulgation of any standard or guideline under this section shall occur not later than 6 months after the date of submission of the proposed standard to the Secretary of Commerce by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

''(f) NOTICE AND COMMENT.—A decision by the Secretary of Commerce to significantly modify, or not promulgate, a proposed standard submitted to the Secretary by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) shall be made after the public is given an opportunity to comment on the Secretary's proposed decision.

''(g) DEFINITIONS.—In this section:

''(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' has the meaning given the term in section 3552 of title 44.

''(2) INFORMATION SECURITY.—The term 'information security' has the meaning given the term in section 3552 of title 44.

''(3) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 3552 of title 44.''.

SEC. 203. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 204. TECHNICAL AND CONFORMING AMENDMENTS.

Section 21(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)) is amended—

(1) in paragraph (2), by striking ''and the Director of the Office of Management and Budget'' and inserting '', the Secretary of Commerce, and the Secretary of Homeland Security''; and

(2) in paragraph (3), by inserting '', the Secretary of Homeland Security,'' after ''the Secretary of Commerce''.

SEC. 205. CLARIFICATION OF AUTHORITIES.

Nothing in this title shall be construed to convey any new regulatory authority to any government entity implementing or complying with any provision of this title.

TITLE III—CRIMINAL PENALTIES

SEC. 301. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended to read as follows:

''(c) The punishment for an offense under subsection (a) or (b) of this section is—

''(1) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(1) of this section;

''(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than 3 years, or both, in the case of an offense under subsection (a)(2); or

''(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2) of this section, if—

''(i) the offense was committed for purposes of commercial advantage or private financial gain;

''(ii) the offense was committed in the furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States, or of any State; or

''(iii) the value of the information obtained, or that would have been obtained if the offense was completed, exceeds $5,000;

''(3) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(3) of this section;

''(4) a fine under this title or imprisonment of not more than 20 years, or both, in the case of an offense under subsection (a)(4) of this section;

''(5)(A) except as provided in subparagraph (C), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A) of this section, if the offense caused—

''(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

''(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

''(iii) physical injury to any person;

''(iv) a threat to public health or safety;

''(v) damage affecting a computer used by, or on behalf of, an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

''(vi) damage affecting 10 or more protected computers during any 1-year period;

''(B) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(B), if the offense caused a harm provided in clause (i) through (vi) of subparagraph (A) of this subsection;

''(C) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both;

''(D) a fine under this title, imprisonment for not more than 10 years, or both, for any other offense under subsection (a)(5);

''(E) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(6) of this section; or

''(F) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(7) of this section.''.

SEC. 302. TRAFFICKING IN PASSWORDS.

Section 1030(a)(6) of title 18, United States Code, is amended to read as follows:

''(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information or means of access through which a protected computer (as defined in subparagraphs (A) and (B) of subsection (e)(2)) may be accessed without authorization.''.

SEC. 303. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD OFFENSES.

Section 1030(b) of title 18, United States Code, is amended by inserting ''as if for the completed offense'' after ''punished as provided''.

SEC. 304. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended by striking subsections (i) and (j) and inserting the following:

''(i) CRIMINAL FORFEITURE.—

''(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

''(A) such persons interest in any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

''(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

''(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

''(j) CIVIL FORFEITURE.—

''(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them:

''(A) Any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

''(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

''(2) Seizures and forfeitures under this subsection shall be governed by the provisions in chapter 46 relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.''.

SEC. 305. DAMAGE TO CRITICAL INFRASTRUCTURE COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) DEFINITIONS.—In this section—

''(1) the term 'computer' has the meaning given the term in section 1030;

''(2) the term 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated, including—

''(A) oil and gas production, storage, conversion, and delivery systems;

''(B) water supply systems;

''(C) telecommunication networks;

''(D) electrical power generation and delivery systems;

''(E) finance and banking systems;

''(F) emergency services;

''(G) transportation systems and services; and

''(H) government operations that provide essential services to the public; and

''(3) the term 'damage' has the meaning given the term in section 1030.

''(b) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer if the damage results in (or, in the case of an attempt, if completed, would have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with the computer.

''(c) PENALTY.—Any person who violates subsection (b) shall be—

''(1) fined under this title;

''(2) imprisoned for not less than 3 years but not more than 20 years; or

''(3) penalized under paragraphs (1) and (2).

''(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place on probation any person convicted of a violation of this section;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for a felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the

court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The chapter analysis for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. 306. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.

Section 1030(e)(6) of title 18, United States Code, is amended by striking ''alter;'' and inserting ''alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;''.

SEC. 307. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

TITLE IV—CYBERSECURITY RESEARCH AND DEVELOPMENT

SEC. 401. NATIONAL HIGH-PERFORMANCE COMPUTING PROGRAM PLANNING AND COORDINATION.

(a) GOALS AND PRIORITIES.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(d) GOALS AND PRIORITIES.—The goals and priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include—

''(1) encouraging and supporting mechanisms for interdisciplinary research and development in networking and information technology, including—

''(A) through collaborations across agencies;

''(B) through collaborations across Program Component Areas;

''(C) through collaborations with industry;

''(D) through collaborations with institutions of higher education;

''(E) through collaborations with Federal laboratories (as defined in section 4 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3703)); and

''(F) through collaborations with international organizations;

''(2) addressing national, multi-agency, multi-faceted challenges of national importance; and

''(3) fostering the transfer of research and development results into new technologies and applications for the benefit of society.''.

(b) DEVELOPMENT OF STRATEGIC PLAN.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(e) STRATEGIC PLAN.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the agencies under subsection (a)(3)(B), working through the National Science and Technology Council and with the assistance of the Office of Science and Technology Policy shall develop a 5-year strategic plan to guide the activities under subsection (a)(1).

''(2) CONTENTS.—The strategic plan shall specify—

''(A) the near-term objectives for the Program;

''(B) the long-term objectives for the Program;

''(C) the anticipated time frame for achieving the near-term objectives;

''(D) the metrics that will be used to assess any progress made toward achieving the near-term objectives and the long-term objectives; and

''(E) how the Program will achieve the goals and priorities under subsection (d).

''(3) IMPLEMENTATION ROADMAP.—

''(A) IN GENERAL.—The agencies under subsection (a)(3)(B) shall develop and annually update an implementation roadmap for the strategic plan.

''(B) REQUIREMENTS.—The information in the implementation roadmap shall be coordinated with the database under section 102(c) and the annual report under section 101(a)(3). The implementation roadmap shall—

''(i) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated, with consideration of any relevant recommendations of the advisory committee;

''(ii) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

''(iii) estimate the funding required for each major research objective of the strategic plan for the next 3 fiscal years.

''(4) RECOMMENDATIONS.—The agencies under subsection (a)(3)(B) shall take into consideration when developing the strategic plan under paragraph (1) the recommendations of—

''(A) the advisory committee under subsection (b); and

''(B) the stakeholders under section 102(a)(3).

''(5) REPORT TO CONGRESS.—The Director of the Office of Science and Technology Policy shall transmit the strategic plan under this subsection, including the implementation roadmap and any updates under paragraph (3), to—

''(A) the advisory committee under subsection (b);

''(B) the Committee on Commerce, Science, and Transportation of the Senate; and

''(C) the Committee on Science and Technology of the House of Representatives.''.

(c) PERIODIC REVIEWS.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(f) PERIODIC REVIEWS.—The agencies under subsection (a)(3)(B) shall—

''(1) periodically assess the contents and funding levels of the Program Component Areas and restructure the Program when warranted, taking into consideration any relevant recommendations of the advisory committee under subsection (b); and

''(2) ensure that the Program includes national, multi-agency, multi-faceted research and development activities, including activities described in section 104.''.

(d) ADDITIONAL RESPONSIBILITIES OF DIRECTOR.—Section 101(a)(2) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)) is amended—

(1) by redesignating subparagraphs (E) and (F) as subparagraphs (G) and (H), respectively; and

(2) by inserting after subparagraph (D) the following:

''(E) encourage and monitor the efforts of the agencies participating in the Program to allocate the level of resources and management attention necessary—

''(i) to ensure that the strategic plan under subsection (e) is developed and executed effectively; and

''(ii) to ensure that the objectives of the Program are met;

''(F) working with the Office of Management and Budget and in coordination with the creation of the database under section 102(c), direct the Office of Science and Technology Policy and the agencies participating in the Program to establish a mechanism (consistent with existing law) to track all ongoing and completed research and development projects and associated funding;''.

(e) ADVISORY COMMITTEE.—Section 101(b) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)) is amended—

(1) in paragraph (1)—

(A) by inserting after the first sentence the following: ''The co-chairs of the advisory committee shall meet the qualifications of committee members and may be members of the Presidents Council of Advisors on Science and Technology.''; and

(B) by striking ''high-performance'' in subparagraph (D) and inserting ''high-end''; and

(2) by amending paragraph (2) to read as follows:

''(2) In addition to the duties under paragraph (1), the advisory committee shall conduct periodic evaluations of the funding, management, coordination, implementation, and activities of the Program. The advisory committee shall report its findings and recommendations not less frequently than once every 3 fiscal years to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives. The report shall be submitted in conjunction with the update of the strategic plan.''.

(f) REPORT.—Section 101(a)(3) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)) is amended—

(1) in subparagraph (C)—

(A) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(B) by striking ''each Program Component Area'' and inserting ''each Program Component Area and each research area supported in accordance with section 104'';

(2) in subparagraph (D)—

(A) by striking ''each Program Component Area,'' and inserting ''each Program Component Area and each research area supported in accordance with section 104,'';

(B) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(C) by striking ''and'' after the semicolon;

(3) by redesignating subparagraph (E) as subparagraph (G); and

(4) by inserting after subparagraph (D) the following:

''(E) include a description of how the objectives for each Program Component Area, and the objectives for activities that involve multiple Program Component Areas, relate to the objectives of the Program identified in the strategic plan under subsection (e);

''(F) include—

''(i) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the next fiscal year by category of activity;

''(ii) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the current fiscal year by category of activity; and

''(iii) the amount of funding provided for the Office of Science and Technology Policy for the current fiscal year by each agency participating in the Program; and''.

(g) DEFINITIONS.—Section 4 of the High-Performance Computing Act of 1991 (15 U.S.C. 5503) is amended—

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

(2) by redesignating paragraph (3) as paragraph (6);

(3) by redesignating paragraphs (6) and (7) as paragraphs (7) and (8), respectively;

(4) by inserting before paragraph (2), as redesignated, the following:

''(1) 'cyber-physical systems' means physical or engineered systems whose networking and information technology functions and physical elements are deeply integrated and are actively connected to the physical world through sensors, actuators, or other means to perform monitoring and control functions;'';

(5) in paragraph (3), as redesignated, by striking ''high-performance computing'' and inserting ''networking and information technology'';

(6) in paragraph (6), as redesignated—

(A) by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(B) by striking ''supercomputer'' and inserting ''high-end computing'';

(7) in paragraph (5), by striking ''network referred to as'' and all that follows through the semicolon and inserting ''network, including advanced computer networks of Federal agencies and departments''; and

(8) in paragraph (7), as redesignated, by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program''.

SEC. 402. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

(a) RESEARCH IN AREAS OF NATIONAL IMPORTANCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.) is amended by adding at the end the following:

''SEC. 104. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

''(a) IN GENERAL.—The Program shall encourage agencies under section 101(a)(3)(B) to support, maintain, and improve national, multi-agency, multi-faceted, research and development activities in networking and information technology directed toward application areas that have the potential for significant contributions to national economic competitiveness and for other significant societal benefits.

''(b) TECHNICAL SOLUTIONS.—An activity under subsection (a) shall be designed to advance the development of research discoveries by demonstrating technical solutions to important problems in areas including—

''(1) cybersecurity;

''(2) health care;

''(3) energy management and low-power systems and devices;

''(4) transportation, including surface and air transportation;

''(5) cyber-physical systems;

''(6) large-scale data analysis and modeling of physical phenomena;

''(7) large scale data analysis and modeling of behavioral phenomena;

''(8) supply chain quality and security; and

''(9) privacy protection and protected disclosure of confidential data.

''(c) RECOMMENDATIONS.—The advisory committee under section 101(b) shall make recommendations to the Program for candidate research and development areas for support under this section.

''(d) CHARACTERISTICS.—

''(1) IN GENERAL.—Research and development activities under this section—

''(A) shall include projects selected on the basis of applications for support through a competitive, merit-based process;

''(B) shall leverage, when possible, Federal investments through collaboration with related State initiatives;

''(C) shall include a plan for fostering the transfer of research discoveries and the results of technology demonstration activities, including from institutions of higher education and Federal laboratories, to industry for commercial development;

''(D) shall involve collaborations among researchers in institutions of higher education and industry; and

''(E) may involve collaborations among nonprofit research institutions and Federal laboratories, as appropriate.

''(2) COST-SHARING.—In selecting applications for support, the agencies under section 101(a)(3)(B) shall give special consideration to projects that include cost sharing from non-Federal sources.

''(3) MULTIDISCIPLINARY RESEARCH CENTERS.—Research and development activities under this section shall be supported through multidisciplinary research centers, including Federal laboratories, that are organized to investigate basic research questions and carry out technology demonstration activities in areas described in subsection (a). Research may be carried out through existing multidisciplinary centers, including those authorized under section 7024(b)(2) of the America COMPETES Act (42 U.S.C. 1862o–10(2)).''.

(b) CYBER-PHYSICAL SYSTEMS.—Section 101(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

''(J) provide for increased understanding of the scientific principles of cyber-physical systems and improve the methods available for the design, development, and operation of cyber-physical systems that are characterized by high reliability, safety, and security; and

''(K) provide for research and development on human-computer interactions, visualization, and big data.''.

(c) TASK FORCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.), as amended by section 402(a) of this Act, is amended by adding at the end the following:

''SEC. 105. TASK FORCE.

''(a) ESTABLISHMENT.—Not later than 180 days after the date of enactment the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy under section 102 shall convene a task force to explore mechanisms for carrying out collaborative research and development activities for cyber-physical systems (including the related technologies required to enable these systems) through a consortium or other appropriate entity with participants from institutions of higher education, Federal laboratories, and industry.

''(b) FUNCTIONS.—The task force shall—

''(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

''(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration and to ensure the development of related scientific and technological milestones;

''(3) define the roles and responsibilities for the participants from institutions of higher education, Federal laboratories, and industry in such entity;

''(4) propose guidelines for assigning intellectual property rights and for transferring research results to the private sector; and

''(5) make recommendations for how such entity could be funded from Federal, State, and non-governmental sources.

''(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education and from industry with knowledge and expertise in cyber-physical systems, and may appoint not more than 2 individuals from Federal laboratories.

''(d) REPORT.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy shall transmit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives a report describing the findings and recommendations of the task force.

''(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

''(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.''.

SEC. 403. PROGRAM IMPROVEMENTS.

Section 102 of the High-Performance Computing Act of 1991 (15 U.S.C. 5512) is amended to read as follows:

''SEC. 102. PROGRAM IMPROVEMENTS.

''(a) FUNCTIONS.—The Director of the Office of Science and Technology Policy shall continue—

''(1) to provide technical and administrative support to—

''(A) the agencies participating in planning and implementing the Program, including support needed to develop the strategic plan under section 101(e); and

''(B) the advisory committee under section 101(b);

''(2) to serve as the primary point of contact on Federal networking and information technology activities for government agencies, academia, industry, professional societies, State computing and networking technology programs, interested citizen groups, and others to exchange technical and programmatic information;

''(3) to solicit input and recommendations from a wide range of stakeholders during the development of each strategic plan under section 101(e) by convening at least 1 workshop with invitees from academia, industry, Federal laboratories, and other relevant organizations and institutions;

''(4) to conduct public outreach, including the dissemination of the advisory committee's findings and recommendations, as appropriate;

''(5) to promote access to and early application of the technologies, innovations, and expertise derived from Program activities to agency missions and systems across the Federal Government and to United States industry;

''(6) to ensure accurate and detailed budget reporting of networking and information technology research and development investment; and

''(7) to encourage agencies participating in the Program to use existing programs and

resources to strengthen networking and information technology education and training, and increase participation in such fields, including by women and underrepresented minorities.

''(b) SOURCE OF FUNDING.—

''(1) IN GENERAL.—The functions under this section shall be supported by funds from each agency participating in the Program.

''(2) SPECIFICATIONS.—The portion of the total budget of the Office of Science and Technology Policy that is provided by each agency participating in the Program for each fiscal year shall be in the same proportion as each agency's share of the total budget for the Program for the previous fiscal year, as specified in the database under section 102(c).

''(c) DATABASE.—

''(1) IN GENERAL.—The Director of the Office of Science and Technology Policy shall develop and maintain a database of projects funded by each agency for the fiscal year for each Program Component Area.

''(2) PUBLIC ACCESSIBILITY.—The Director of the Office of Science and Technology Policy shall make the database accessible to the public.

''(3) DATABASE CONTENTS.—The database shall include, for each project in the database—

''(A) a description of the project;

''(B) each agency, industry, institution of higher education, Federal laboratory, or international institution involved in the project;

''(C) the source funding of the project (set forth by agency);

''(D) the funding history of the project; and

''(E) whether the project has been completed.''.

SEC. 404. IMPROVING EDUCATION OF NETWORKING AND INFORMATION TECHNOLOGY, INCLUDING HIGH PERFORMANCE COMPUTING.

Section 201(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)) is amended—

(1) by redesignating paragraphs (2) through (4) as paragraphs (3) through (5), respectively; and

(2) by inserting after paragraph (1) the following:

''(2) the National Science Foundation shall use its existing programs, in collaboration with other agencies, as appropriate, to improve the teaching and learning of networking and information technology at all levels of education and to increase participation in networking and information technology fields;''.

SEC. 405. CONFORMING AND TECHNICAL AMENDMENTS TO THE HIGH-PERFORMANCE COMPUTING ACT OF 1991.

(a) SECTION 3.—Section 3 of the High-Performance Computing Act of 1991 (15 U.S.C. 5502) is amended—

(1) in the matter preceding paragraph (1), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(2) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(B) in subparagraphs (A), (F), and (G), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(C) in subparagraph (H), by striking ''high-performance'' and inserting ''high-end''; and

(3) in paragraph (2)—

(A) by striking ''high-performance computing and'' and inserting ''networking and information technology, and''; and

(B) by striking ''high-performance computing network'' and inserting ''networking and information technology''.

(b) TITLE HEADING.—The heading of title I of the High-Performance Computing Act of 1991 (105 Stat. 1595) is amended by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''.

(c) SECTION 101.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT**'';

(2) in subsection (a)—

(A) in the subsection heading, by striking ''NATIONAL HIGH-PERFORMANCE COMPUTING'' and inserting ''NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT'';

(B) in paragraph (1)—

(i) by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program'';

(ii) in subparagraph (A), by striking ''high-performance computing, including networking'' and inserting ''networking and information technology'';

(iii) in subparagraphs (B) and (G), by striking ''high-performance'' each place it appears and inserting ''high-end''; and

(iv) in subparagraph (C), by striking ''high-performance computing and networking'' and inserting ''high-end computing, distributed, and networking''; and

(C) in paragraph (2)—

(i) in subparagraphs (A) and (C)—

(I) by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(II) by striking ''development, networking,'' each place it appears and inserting ''development,''; and

(ii) in subparagraphs (G) and (H), as redesignated by section 401(d) of this Act, by striking ''high-performance'' each place it appears and inserting ''high-end'';

(3) in subsection (b)(1), in the matter preceding subparagraph (A), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(4) in subsection (c)(1)(A), by striking ''high-performance computing'' and inserting ''networking and information technology''.

(d) SECTION 201.—Section 201(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)(1)) is amended by striking ''high-performance computing and advanced high-speed computer networking'' and inserting ''networking and information technology research and development''.

(e) SECTION 202.—Section 202(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5522(a)) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(f) SECTION 203.—Section 203(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5523(a)) is amended—

(1) in paragraph (1), by striking ''high-performance computing and networking'' and inserting ''networking and information technology''; and

(2) in paragraph (2)(A), by striking ''high-performance'' and inserting ''high-end''.

(g) SECTION 204.—Section 204 of the High-Performance Computing Act of 1991 (15 U.S.C. 5524) is amended—

(1) in subsection (a)(1)—

(A) in subparagraph (A), by striking ''high-performance computing systems and networks'' and inserting ''networking and information technology systems and capabilities'';

(B) in subparagraph (B), by striking ''interoperability of high-performance computing systems in networks and for common user interfaces to systems'' and inserting ''interoperability and usability of networking and information technology systems''; and

(C) in subparagraph (C), by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(2) in subsection (b)—

(A) by striking ''HIGH-PERFORMANCE COMPUTING AND NETWORK'' in the heading and inserting ''NETWORKING AND INFORMATION TECHNOLOGY''; and

(B) by striking ''sensitive''.

(h) SECTION 205.—Section 205(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5525(a)) is amended by striking ''computational'' and inserting ''networking and information technology''.

(i) SECTION 206.—Section 206(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5526(a)) is amended by striking ''computational research'' and inserting ''networking and information technology research''.

(j) SECTION 207.—Section 207 of the High-Performance Computing Act of 1991 (15 U.S.C. 5527) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(k) SECTION 208.—Section 208 of the High-Performance Computing Act of 1991 (15 U.S.C. 5528) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''; and

(2) in subsection (a)—

(A) in paragraph (1), by striking ''High-performance computing and associated'' and inserting ''Networking and information'';

(B) in paragraph (2), by striking ''high-performance computing'' and inserting ''networking and information technologies'';

(C) in paragraph (3), by striking ''high-performance'' and inserting ''high-end'';

(D) in paragraph (4), by striking ''high-performance computers and associated'' and inserting ''networking and information''; and

(E) in paragraph (5), by striking ''high-performance computing and associated'' and inserting ''networking and information''.

SEC. 406. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with the Secretary of Homeland Security, shall carry out a Federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals and security managers to meet the needs of the cybersecurity mission for the Federal government.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The program shall—

(1) annually assess the workforce needs of the Federal government for cybersecurity professionals, including network engineers, software engineers, and other experts in order to determine how many scholarships should be awarded annually to ensure that the workforce needs following graduation match the number of scholarships awarded;

(2) provide scholarships for up to 1,000 students per year in their pursuit of undergraduate or graduate degrees in the cybersecurity field, in an amount that may include coverage for full tuition, fees, and a stipend;

(3) require each scholarship recipient, as a condition of receiving a scholarship under the program, to serve in a Federal information technology workforce for a period equal to one and one-half times each year, or partial year, of scholarship received, in addition to an internship in the cybersecurity field, if applicable, following graduation;

(4) provide a procedure for the National Science Foundation or a Federal agency, consistent with regulations of the Office of

Personnel Management, to request and fund a security clearance for a scholarship recipient, including providing for clearance during a summer internship and upon graduation; and

(5) provide opportunities for students to receive temporary appointments for meaningful employment in the Federal information technology workforce during school vacation periods and for internships.

(c) HIRING AUTHORITY.—

(1) IN GENERAL.—For purposes of any law or regulation governing the appointment of an individual in the Federal civil service, upon the successful completion of the student's studies, a student receiving a scholarship under the program may—

(A) be hired under section 213.3102(r) of title 5, Code of Federal Regulations; and

(B) be exempt from competitive service.

(2) COMPETITIVE SERVICE.—Upon satisfactory fulfillment of the service term under paragraph (1), an individual may be converted to a competitive service position without competition if the individual meets the requirements for that position.

(d) ELIGIBILITY.—The eligibility requirements for a scholarship under this section shall include that a scholarship applicant—

(1) be a citizen of the United States;

(2) be eligible to be granted a security clearance;

(3) maintain a grade point average of 3.2 or above on a 4.0 scale for undergraduate study or a 3.5 or above on a 4.0 scale for postgraduate study;

(4) demonstrate a commitment to a career in improving the security of the information infrastructure; and

(5) has demonstrated a level of proficiency in math or computer sciences.

(e) FAILURE TO COMPLETE SERVICE OBLIGATION.—

(1) IN GENERAL.—A scholarship recipient under this section shall be liable to the United States under paragraph (2) if the scholarship recipient—

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

(C) withdraws from the program for which the award was made before the completion of such program;

(D) declares that the individual does not intend to fulfill the service obligation under this section;

(E) fails to fulfill the service obligation of the individual under this section; or

(F) loses a security clearance or becomes ineligible for a security clearance.

(2) REPAYMENT AMOUNTS.—

(A) LESS THAN 1 YEAR OF SERVICE.—If a circumstance under paragraph (1) occurs before the completion of 1 year of a service obligation under this section, the total amount of awards received by the individual under this section shall be repaid.

(B) ONE OR MORE YEARS OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid.

(f) EVALUATION AND REPORT.—The Director of the National Science Foundation shall—

(1) evaluate the success of recruiting individuals for scholarships under this section and of hiring and retaining those individuals in the public sector workforce, including the annual cost and an assessment of how the program actually improves the Federal workforce; and

(2) periodically report the findings under paragraph (1) to Congress.

(g) AUTHORIZATION OF APPROPRIATIONS.—From amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), the Director may use funds to carry out the requirements of this section for fiscal years 2012 through 2013.

SEC. 407. STUDY AND ANALYSIS OF CERTIFICATION AND TRAINING OF INFORMATION INFRASTRUCTURE PROFESSIONALS.

(a) STUDY.—The President shall enter into an agreement with the National Academies to conduct a comprehensive study of government, academic, and private-sector accreditation, training, and certification programs for personnel working in information infrastructure. The agreement shall require the National Academies to consult with sector coordinating councils and relevant governmental agencies, regulatory entities, and nongovernmental organizations in the course of the study.

(b) SCOPE.—The study shall include—

(1) an evaluation of the body of knowledge and various skills that specific categories of personnel working in information infrastructure should possess in order to secure information systems;

(2) an assessment of whether existing government, academic, and private-sector accreditation, training, and certification programs provide the body of knowledge and various skills described in paragraph (1);

(3) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibility; and

(4) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the National Academies shall submit to the President and Congress a report on the results of the study. The report shall include—

(1) findings regarding the state of information infrastructure accreditation, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for the improvement of information infrastructure accreditation, training, and certification programs.

SEC. 408. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

(a) IN GENERAL.—The Director of the National Institute of Standards and Technology, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.

(b) CONSULTATION WITH THE PRIVATE SECTOR.—In carrying out the activities under subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

SEC. 409. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director of the National Institute of Standards and Technology shall continue a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen authentication methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

SEC. 410. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY RESEARCH GRANT AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking ''property.'' and inserting ''property;''; and

(3) by adding at the end the following:

''(J) secure fundamental protocols that are at the heart of inter-network communications and data exchange;

''(K) system security that addresses the building of secure systems from trusted and untrusted components;

''(L) monitoring and detection; and

''(M) resiliency and rapid recovery methods.''.

(b) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY GRANTS.—Section 4(a)(3) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(3)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(c) COMPUTER AND NETWORK SECURITY CENTERS.—Section 4(b)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7403(b)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)(6)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of the Cyber Security Research and Development Act (15 U.S.C. 7404(b)(2)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—Section 5(c)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7404(c)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

SA 2693. Mr. COATS submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 118, line 16, insert '', including legal and behavioral impediments to deployment of proven security policies'' before the semicolon.

SA 2694. Mr. COATS submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 118, line 25, strike ''and'' and all that follows through page 119, line 2, and insert the following:

(7) affiliation with existing research programs of the Federal Government;

(8) demonstrated expertise in cybersecurity law, including the legal impediments to adoption of proven security processes; and

(9) demonstrated expertise in social and behavioral research that can assist in developing policies and incentives to help protect against cyber attacks.

SA 2695. Mr. SESSIONS submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. NOTICE REQUIRED PRIOR TO TRANSFER OF CERTAIN INDIVIDUALS DETAINED AT THE DETENTION FACILITY AT PARWAN, AFGHANISTAN.

(a) NOTICE REQUIRED.—The Secretary of Defense shall submit to the appropriate congressional committees notice in writing of the proposed transfer of any individual detained pursuant to the Authorization for Use of Military Force (Public Law 107–40; 50 U.S.C. 1541 note) who is a national of a country other than the United States or Afghanistan from detention at the Detention Facility at Parwan, Afghanistan, to the custody of the Government of Afghanistan or of any other country. Such notice shall be provided not later than 10 days before such a transfer may take place.

(b) ADDITIONAL ASSESSMENTS AND CERTIFICATIONS.—As part of the notice required under subsection (a), the Secretary shall include the following:

(1) In the case of the proposed transfer of such an individual by reason of the individual being released, an assessment of the threat posed by the individual and the security environment of the country to which the individual is to be transferred.

(2) In the case of the proposed transfer of such an individual to a country other than Afghanistan for the purpose of the prosecution of the individual, a certification that an assessment has been conducted regarding the capacity, willingness, and historical track record of the country with respect to prosecuting similar cases, including a description of the evidence against the individual that is likely to be admissible as part of the prosecution.

(3) In the case of the proposed transfer of such an individual for reintegration or rehabilitation in a country other than Afghanistan, a certification that an assessment has been conducted regarding the capacity, willingness, and historical track record of the country for reintegrating or rehabilitating similar individuals.

(4) In the case of the proposed transfer of such an individual to the custody of the government of Afghanistan for prosecution or detention, a certification that an assessment has been conducted regarding the capacity, willingness, and historical track record of Afghanistan to prosecute or detain long-term such individuals.

(c) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term ''appropriate congressional committees'' means—

(1) the Committee on Armed Services and the Committee on Foreign Affairs of the House of Representatives; and

(2) the Committee on Armed Services and the Committee on Foreign Relations of the Senate.

SA 2696. Mr. MCCAIN (for himself, Mrs. HUTCHISON, Mr. CHAMBLISS, Mr. GRASSLEY, Ms. MURKOWSKI, Mr. COATS, Mr. BURR, and Mr. JOHNSON of Wisconsin) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 1, strike line 4 and all that follows and insert the following:

(a) SHORT TITLE.—This Act may be cited as the ''Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012'' or ''SECURE IT''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

TITLE I—FACILITATING SHARING OF CYBER THREAT INFORMATION

SEC. 101. DEFINITIONS.

In this title:

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

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

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

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

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

(3) COUNTERMEASURE.—The term ''countermeasure'' means an automated or a manual action with defensive intent to mitigate cyber threats.

(4) CYBER THREAT INFORMATION.—The term ''cyber threat information'' means information that indicates or describes—

(A) a technical or operation vulnerability or a cyber threat mitigation measure;

(B) an action or operation to mitigate a cyber threat;

(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

(D) a method of defeating a technical control;

(E) a method of defeating an operational control;

(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

(G) 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 inadvertently enable the defeat of a technical or operational control;

(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

(J) any combination of subparagraphs (A) through (I).

(5) CYBERSECURITY CENTER.—The term ''cybersecurity center'' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

(6) CYBERSECURITY SYSTEM.—The term ''cybersecurity system'' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or to safeguard, a system or network, including measures intended to protect a system or network from—

(A) efforts to degrade, disrupt, or destroy such system or network; or

(B) theft or misappropriations of private or government information, intellectual property, or personally identifiable information.

(7) ENTITY.—

(A) IN GENERAL.—The term ''entity'' means any private entity, non-Federal government agency or department, or State, tribal, or local government agency or department (including an officer, employee, or agent thereof).

(B) INCLUSIONS.—The term ''entity'' includes a government agency or department (including an officer, employee, or agent thereof) 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.

(8) FEDERAL INFORMATION SYSTEM.—The term ''Federal information system'' means an information system of a Federal department or agency used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

(9) INFORMATION SECURITY.—The term ''information security'' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

(C) availability, by ensuring timely and reliable access to and use of information.

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

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

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

(13) OPERATIONAL CONTROL.—The term ''operational control'' means a security control for an information system that primarily is implemented and executed by people.

(14) OPERATIONAL VULNERABILITY.—The term ''operational vulnerability'' means any attribute of policy, process, or procedure that could enable or facilitate the defeat of an operational control.

(15) PRIVATE ENTITY.—The term ''private entity'' means any individual or any private group, organization, or corporation, including an officer, employee, or agent thereof.

(16) SIGNIFICANT CYBER INCIDENT.—The term ''significant cyber incident'' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

(17) TECHNICAL CONTROL.—The term ''technical control'' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

(18) TECHNICAL VULNERABILITY.—The term ''technical vulnerability'' means any attribute of hardware or software that could enable or facilitate the defeat of a technical control.

(19) 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. 102. AUTHORIZATION TO SHARE CYBER THREAT INFORMATION.

(a) VOLUNTARY DISCLOSURE.—

(1) PRIVATE ENTITIES.—Notwithstanding any other provision of law, a private entity may, for the purpose of preventing, investigating, or otherwise mitigating threats to information security, on its own networks, or as authorized by another entity, on such entity's networks, employ countermeasures and use cybersecurity systems in order to obtain, identify, or otherwise possess cyber threat information.

(2) ENTITIES.—Notwithstanding any other provision of law, an entity may disclose cyber threat information to—

(A) a cybersecurity center; or

(B) any other entity in order to assist with preventing, investigating, or otherwise mitigating threats to information security.

(3) INFORMATION SECURITY PROVIDERS.—If the cyber threat information described in paragraph (1) is obtained, identified, or otherwise possessed in the course of providing information security products or services under contract to another entity, that entity shall be given, at any time prior to disclosure of such information, a reasonable opportunity to authorize or prevent such disclosure, to request anonymization of such information, or to request that reasonable efforts be made to safeguard such information that identifies specific persons from unauthorized access or disclosure.

(b) SIGNIFICANT CYBER INCIDENTS INVOLVING FEDERAL INFORMATION SYSTEMS.—

(1) IN GENERAL.—An entity providing electronic communication services, remote computing services, or information security services to a Federal department or agency shall inform the Federal department or agency of a significant cyber incident involving the Federal information system of that Federal department or agency that—

(A) is directly known to the entity as a result of providing such services;

(B) is directly related to the provision of such services by the entity; and

(C) as determined by the entity, has impeded or will impede the performance of a critical mission of the Federal department or agency.

(2) ADVANCE COORDINATION.—A Federal department or agency receiving the services described in paragraph (1) shall coordinate in advance with an entity described in paragraph (1) to develop the parameters of any information that may be provided under paragraph (1), including clarification of the type of significant cyber incident that will impede the performance of a critical mission of the Federal department or agency.

(3) REPORT.—A Federal department or agency shall report information provided under this subsection to a cybersecurity center.

(4) CONSTRUCTION.—Any information provided to a cybersecurity center under paragraph (3) shall be treated in the same manner as information provided to a cybersecurity center under subsection (a).

(c) INFORMATION SHARED WITH OR PROVIDED TO A CYBERSECURITY CENTER.—Cyber threat information provided to a cybersecurity center under this section—

(1) may be disclosed to, retained by, and used by, consistent with otherwise applicable Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal government for a cybersecurity purpose, a national security purpose, or in order to prevent, investigate, or prosecute any of the offenses listed in section 2516 of title 18, United States Code, and such information shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under this paragraph;

(2) may, with the prior written consent of the entity submitting such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(3) shall be considered the commercial, financial, or proprietary information of the entity providing such information to the Federal government and any disclosure outside the Federal government may only be made upon the prior written consent by such entity and shall not constitute a waiver of any applicable privilege or protection provided by law, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent;

(4) shall be 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;

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

(6) shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official;

(7) shall not, if subsequently provided to a State, tribal, or local government or government agency, otherwise be disclosed or distributed to any entity by such State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except that if the need for immediate disclosure prevents obtaining written consent, such consent may be provided orally with subsequent documentation of such consent; and

(8) shall not be directly used by any Federal, State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this paragraph.

(d) PROCEDURES RELATING TO INFORMATION SHARING WITH A CYBERSECURITY CENTER.—Not later than 60 days after the date of enactment of this Act, the heads of each department or agency containing a cybersecurity center shall jointly develop, promulgate, and submit to Congress procedures to ensure that cyber threat information shared with or provided to—

(1) a cybersecurity center under this section—

(A) may be submitted to a cybersecurity center by an entity, to the greatest extent possible, through a uniform, publicly available process or format that is easily accessible on the website of such cybersecurity center, and that includes the ability to provide relevant details about the cyber threat information and written consent to any subsequent disclosures authorized by this paragraph;

(B) shall immediately be further shared with each cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government;

(C) is handled by the Federal government in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title, and the Federal government may undertake efforts consistent with this subparagraph to limit the impact on privacy and civil liberties of the sharing of cyber threat information with the Federal government; and

(D) except as provided in this section, shall only be used, disclosed, or handled in accordance with the provisions of subsection (c); and

(2) a Federal agency or department under subsection (b) is provided immediately to a cybersecurity center in order to prevent, investigate, or otherwise mitigate threats to information security across the Federal government.

(e) INFORMATION SHARED BETWEEN ENTITIES.—

(1) IN GENERAL.—An entity sharing cyber threat information with another entity under this title may restrict the use or sharing of such information by such other entity.

(2) FURTHER SHARING.—Cyber threat information shared by any entity with another entity under this title—

(A) shall only be further shared in accordance with any restrictions placed on the sharing of such information by the entity authorizing such sharing, such as appropriate anonymization of such information; and

(B) may not be used by any entity to gain an unfair competitive advantage to the detriment of the entity authorizing the sharing of such information, except that the conduct described in paragraph (3) shall not constitute unfair competitive conduct.

(3) INFORMATION SHARED WITH STATE, TRIBAL, OR LOCAL GOVERNMENT OR GOVERNMENT AGENCY.—Cyber threat information shared with a State, tribal, or local government or government agency under this title—

(A) may, with the prior written consent of the entity sharing such information, be disclosed to and used by a State, tribal, or local government or government agency for the purpose of protecting information systems, or in furtherance of preventing, investigating, or prosecuting a criminal act, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent;

(B) shall be deemed voluntarily shared information and exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records;

(C) shall not be disclosed or distributed to any entity by the State, tribal, or local government or government agency without the prior written consent of the entity submitting such information, notwithstanding any State, tribal, or local law requiring disclosure of information or records, except if the need for immediate disclosure prevents obtaining written consent, consent may be provided orally with subsequent documentation of the consent; and

(D) shall not be directly used by any State, tribal, or local department or agency to regulate the lawful activities of an entity, including activities relating to obtaining, identifying, or otherwise possessing cyber threat information, except that the procedures required to be developed and implemented under this title shall not be considered regulations within the meaning of this subparagraph.

(4) ANTITRUST EXEMPTION.—The exchange or provision of cyber threat information or assistance between 2 or more private entities under this title shall not be considered a violation of any provision of antitrust laws if exchanged or provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of threats to information security; or

(B) communicating or disclosing of cyber threat information to help prevent, investigate or otherwise mitigate the effects of a threat to information security.

(5) NO RIGHT OR BENEFIT.—The provision of cyber threat information to an entity under this section shall not create a right or a benefit to similar information by such entity or any other entity.

(f) FEDERAL PREEMPTION.—

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

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

(3) PUBLIC DISCLOSURE.—No information shared with or provided to a State, tribal, or local government or government agency pursuant to this section shall be made publicly available pursuant to any State, tribal, or local law requiring disclosure of information or records.

(g) CIVIL AND CRIMINAL LIABILITY.—

(1) GENERAL PROTECTIONS.—

(A) PRIVATE ENTITIES.—No cause of action shall lie or be maintained in any court against any private entity for—

(i) the use of countermeasures and cybersecurity systems as authorized by this title;

(ii) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(iii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such private entity.

(B) ENTITIES.—No cause of action shall lie or be maintained in any court against any entity for—

(i) the use, receipt, or disclosure of any cyber threat information as authorized by this title; or

(ii) the subsequent actions or inactions of any lawful recipient of cyber threat information provided by such entity.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed 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, and use of classified information.

(h) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this section shall be construed to limit or prohibit otherwise lawful disclosures of communications, records, or other information by a private entity to any other governmental or private entity not covered under this section.

(i) WHISTLEBLOWER PROTECTION.—Nothing in this Act shall be construed to preempt or preclude any employee from exercising rights currently provided under any whistleblower law, rule, or regulation.

(j) RELATIONSHIP TO OTHER LAWS.—The submission of cyber threat information under this section to a cybersecurity center shall not affect any requirement under any other provision of law for an entity to provide information to the Federal government.

SEC. 103. INFORMATION SHARING BY THE FEDERAL GOVERNMENT.

(a) CLASSIFIED INFORMATION.—

(1) PROCEDURES.—Consistent with the protection of intelligence sources and methods, and as otherwise determined appropriate, the Director of National Intelligence and the Secretary of Defense, in consultation with the heads of the appropriate Federal departments or agencies, shall develop and promulgate procedures to facilitate and promote—

(A) the immediate sharing, through the cybersecurity centers, of classified cyber threat information in the possession of the Federal government with appropriately cleared representatives of any appropriate entity; and

(B) the declassification and immediate sharing, through the cybersecurity centers, with any entity or, if appropriate, public availability of cyber threat information in the possession of the Federal government;

(2) HANDLING OF CLASSIFIED INFORMATION.—The procedures developed under paragraph (1) shall ensure that each entity receiving classified cyber threat information pursuant to this section has acknowledged in writing the ongoing obligation to comply with all laws, executive orders, and procedures concerning the appropriate handling, disclosure, or use of classified information.

(b) UNCLASSIFIED CYBER THREAT INFORMATION.—The heads of each department or agency containing a cybersecurity center shall jointly develop and promulgate procedures that ensure that, consistent with the provisions of this section, unclassified, including controlled unclassified, cyber threat information in the possession of the Federal government—

(1) is shared, through the cybersecurity centers, in an immediate and adequate manner with appropriate entities; and

(2) if appropriate, is made publicly available.

(c) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed under this section shall incorporate, to the greatest extent possible, existing processes utilized by sector specific information sharing and analysis centers.

(2) COORDINATION WITH ENTITIES.—In developing the procedures required under this section, the Director of National Intelligence and the heads of each department or agency containing a cybersecurity center shall coordinate with appropriate entities to ensure that protocols are implemented that will facilitate and promote the sharing of cyber threat information by the Federal government.

(d) ADDITIONAL RESPONSIBILITIES OF CYBERSECURITY CENTERS.—Consistent with section 102, a cybersecurity center shall—

(1) facilitate information sharing, interaction, and collaboration among and between cybersecurity centers and—

(A) other Federal entities;

(B) any entity; and

(C) international partners, in consultation with the Secretary of State;

(2) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of information systems; and

(3) coordinate with other Federal entities, as appropriate, to integrate information from across the Federal government to provide situational awareness of the cybersecurity posture of the United States.

(e) SHARING WITHIN THE FEDERAL GOVERNMENT.—The heads of appropriate Federal departments and agencies shall ensure that cyber threat information in the possession of such Federal departments or agencies that relates to the prevention, investigation, or mitigation of threats to information security across the Federal government is shared effectively with the cybersecurity centers.

(f) SUBMISSION TO CONGRESS.—Not later than 60 days after the date of enactment of this Act, the Director of National Intelligence, in coordination with the appropriate head of a department or an agency containing a cybersecurity center, shall submit the procedures required by this section to Congress.

SEC. 104. CONSTRUCTION.

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

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

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any entity and the Federal government, except as specified under section 102(b); or

(4) to modify the authority of a department or agency of the Federal government to protect sources and methods and the national security of the United States.

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

(1) to require an entity to share information with the Federal government, except as expressly provided under section 102(b); or

(2) to condition the sharing of cyber threat information with an entity on such entity's provision of cyber threat information to the Federal government.

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

(d) USE AND RETENTION OF INFORMATION.—Nothing in this title shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal government to retain or use any information shared under section 102 for any use other than a use permitted under section 102(c)(1).

(e) NO NEW FUNDING.—An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 105. REPORT ON IMPLEMENTATION.

(a) CONTENT OF REPORT.—Not later than 1 year after the date of enactment of this Act, and biennially thereafter, the heads of each department or agency containing a cybersecurity center shall jointly submit, in coordination with the privacy and civil liberties officials of such departments or agencies and the Privacy and Civil Liberties Oversight Board, a detailed report to Congress concerning the implementation of this title, including—

(1) an assessment of the sufficiency of the procedures developed under section 103 of this Act in ensuring that cyber threat information in the possession of the Federal government is provided in an immediate and adequate manner to appropriate entities or, if appropriate, is made publicly available;

(2) an assessment of whether information has been appropriately classified and an accounting of the number of security clearances authorized by the Federal government for purposes of this title;

(3) a review of the type of cyber threat information shared with a cybersecurity center under section 102 of this Act, including whether such information meets the definition of cyber threat information under section 101, the degree to which such information may impact the privacy and civil liberties of individuals, any appropriate metrics to determine any impact of the sharing of such information with the Federal government on privacy and civil liberties, and the adequacy of any steps taken to reduce such impact;

(4) a review of actions taken by the Federal government based on information provided to a cybersecurity center under section 102 of this Act, including the appropriateness of any subsequent use under section 102(c)(1) of this Act and whether there was inappropriate stovepiping within the Federal government of any such information;

(5) a description of any violations of the requirements of this title by the Federal government;

(6) a classified list of entities that received classified information from the Federal government under section 103 of this Act and a description of any indication that such information may not have been appropriately handled;

(7) a summary of any breach of information security, if known, attributable to a specific failure by any entity or the Federal government to act on cyber threat information in the possession of such entity or the Federal government that resulted in substantial economic harm or injury to a specific entity or the Federal government; and

(8) any recommendation for improvements or modifications to the authorities under this title.

(b) FORM OF REPORT.—The report under subsection (a) shall be submitted in unclassified form, but shall include a classified annex.

SEC. 106. INSPECTOR GENERAL REVIEW.

(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency are authorized to review compliance by the cybersecurity centers, and by any Federal department or agency receiving cyber threat information from such cybersecurity centers, with the procedures required under section 102 of this Act.

(b) SCOPE OF REVIEW.—The review under subsection (a) shall consider whether the Federal government has handled such cyber threat information in a reasonable manner, including consideration of the need to protect the privacy and civil liberties of individuals through anonymization or other appropriate methods, while fully accomplishing the objectives of this title.

(c) REPORT TO CONGRESS.—Each review conducted under this section shall be provided to Congress not later than 30 days after the date of completion of the review.

SEC. 107. TECHNICAL AMENDMENTS.

Section 552(b) of title 5, United States Code, is amended—

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

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

(3) by adding at the end the following:

''(10) information shared with or provided to a cybersecurity center under section 102 of title I of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012.''.

SEC. 108. ACCESS TO CLASSIFIED INFORMATION.

(a) AUTHORIZATION REQUIRED.—No person shall be provided with access to classified information (as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 435 note; relating to classified national security information)) relating to cyber security threats or cyber security vulnerabilities under this title without the appropriate security clearances.

(b) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall, consistent with applicable procedures and requirements, and if otherwise deemed appropriate, assist an individual in timely obtaining an appropriate security clearance where such individual has been determined to be eligible for such clearance and has a need-to-know (as defined in section 6.1 of that Executive Order) classified information to carry out this title.

TITLE II—COORDINATION OF FEDERAL INFORMATION SECURITY POLICY

SEC. 201. COORDINATION OF FEDERAL INFORMATION SECURITY POLICY.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3551. Purposes

''The purposes of this subchapter are—

''(1) to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

''(2) to recognize the highly networked nature of the current Federal computing environment and provide effective government-wide management of policies, directives, standards, and guidelines, as well as effective and nimble oversight of and response to information security risks, including coordination of information security efforts throughout the Federal civilian, national security, and law enforcement communities;

''(3) to provide for development and maintenance of controls required to protect agency information and information systems and contribute to the overall improvement of agency information security posture;

''(4) to provide for the development of tools and methods to assess and respond to real-time situational risk for Federal information system operations and assets; and

''(5) to provide a mechanism for improving agency information security programs

through continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.

"§ 3552. Definitions

''In this subchapter:

''(1) ADEQUATE SECURITY.—The term 'adequate security' means security commensurate with the risk and magnitude of the harm resulting from the unauthorized access to or loss, misuse, destruction, or modification of information.

''(2) AGENCY.—The term 'agency' has the meaning given the term in section 3502 of title 44.

''(3) CYBERSECURITY CENTER.—The term 'cybersecurity center' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the National Cybersecurity and Communications Integration Center, and any successor center.

''(4) CYBER THREAT INFORMATION.—The term 'cyber threat information' means information that indicates or describes—

''(A) a technical or operation vulnerability or a cyber threat mitigation measure;

''(B) an action or operation to mitigate a cyber threat;

''(C) malicious reconnaissance, including anomalous patterns of network activity that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

''(D) a method of defeating a technical control;

''(E) a method of defeating an operational control;

''(F) network activity or protocols known to be associated with a malicious cyber actor or that signify malicious cyber intent;

''(G) 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 inadvertently enable the defeat of a technical or operational control;

''(H) any other attribute of a cybersecurity threat or cyber defense information that would foster situational awareness of the United States cybersecurity posture, if disclosure of such attribute or information is not otherwise prohibited by law;

''(I) the actual or potential harm caused by a cyber incident, including information exfiltrated when it is necessary in order to identify or describe a cybersecurity threat; or

''(J) any combination of subparagraphs (A) through (I).

''(5) DIRECTOR.—The term 'Director' means the Director of the Office of Management and Budget unless otherwise specified.

''(6) ENVIRONMENT OF OPERATION.—The term 'environment of operation' means the information system and environment in which those systems operate, including changing threats, vulnerabilities, technologies, and missions and business practices.

''(7) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

''(8) INCIDENT.—The term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

''(B) constitutes a violation of law or an imminent threat of violation of a law, a security policy, a security procedure, or an acceptable use policy.

''(9) INFORMATION RESOURCES.—The term 'information resources' has the meaning given the term in section 3502 of title 44.

''(10) INFORMATION SECURITY.—The term 'information security' means protecting information and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction in order to provide—

''(A) integrity, by guarding against improper information modification or destruction, including by ensuring information nonrepudiation and authenticity;

''(B) confidentiality, by preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; or

''(C) availability, by ensuring timely and reliable access to and use of information.

''(11) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44.

''(12) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 11101 of title 40.

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

''(14) NATIONAL SECURITY SYSTEM.—

''(A) IN GENERAL.—The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

''(i) the function, operation, or use of which—

''(I) involves intelligence activities;

''(II) involves cryptologic activities related to national security;

''(III) involves command and control of military forces;

''(IV) involves equipment that is an integral part of a weapon or weapons system; or

''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

''(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

''(B) LIMITATION.—Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

''(15) OPERATIONAL CONTROL.—The term 'operational control' means a security control for an information system that primarily is implemented and executed by people.

''(16) PERSON.—The term 'person' has the meaning given the term in section 3502 of title 44.

''(17) SECRETARY.—The term 'Secretary' means the Secretary of Commerce unless otherwise specified.

''(18) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls, including safeguards or countermeasures, prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

''(19) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cyber incident resulting in, or an attempted cyber incident that, if successful, would have resulted in—

''(A) the exfiltration from a Federal information system of data that is essential to the operation of the Federal information system; or

''(B) an incident in which an operational or technical control essential to the security or operation of a Federal information system was defeated.

''(20) TECHNICAL CONTROL.—The term 'technical control' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

"§ 3553. Federal information security authority and coordination

''(a) IN GENERAL.—The Secretary, in consultation with the Secretary of Homeland Security, shall—

''(1) issue compulsory and binding policies and directives governing agency information security operations, and require implementation of such policies and directives, including—

''(A) policies and directives consistent with the standards and guidelines promulgated under section 11331 of title 40 to identify and provide information security protections prioritized and commensurate with the risk and impact resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by or on behalf of an agency; or

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(B) minimum operational requirements for Federal Government to protect agency information systems and provide common situational awareness across all agency information systems;

''(C) reporting requirements, consistent with relevant law, regarding information security incidents and cyber threat information;

''(D) requirements for agencywide information security programs;

''(E) performance requirements and metrics for the security of agency information systems;

''(F) training requirements to ensure that agencies are able to fully and timely comply with the policies and directives issued by the Secretary under this subchapter;

''(G) training requirements regarding privacy, civil rights, and civil liberties, and information oversight for agency information security personnel;

''(H) requirements for the annual reports to the Secretary under section 3554(d);

''(I) any other information security operations or information security requirements as determined by the Secretary in coordination with relevant agency heads; and

''(J) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(2) review the agencywide information security programs under section 3554; and

''(3) designate an individual or an entity at each cybersecurity center, among other responsibilities—

''(A) to receive reports and information about information security incidents, cyber

threat information, and deterioration of security control affecting agency information systems; and

''(B) to act on or share the information under subparagraph (A) in accordance with this subchapter.

''(b) CONSIDERATIONS.—When issuing policies and directives under subsection (a), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology under section 11331 of title 40.

''(c) LIMITATION OF AUTHORITY.—The authorities of the Secretary under this section shall not apply to national security systems. Information security policies, directives, standards and guidelines for national security systems shall be overseen as directed by the President and, in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

''(d) STATUTORY CONSTRUCTION.—Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any head of an agency over such agency.

''§ 3554. Agency responsibilities

''(a) IN GENERAL.—The head of each agency shall—

''(1) be responsible for—

''(A) complying with the policies and directives issued under section 3553;

''(B) providing information security protections commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by the agency or by a contractor of an agency or other organization on behalf of an agency; and

''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(C) complying with the requirements of this subchapter, including—

''(i) information security standards and guidelines promulgated under section 11331 of title 40;

''(ii) for any national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued as directed by the President; and

''(iii) for any non-national security systems operated or controlled by that agency, information security policies, directives, standards and guidelines issued under section 3553;

''(D) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

''(E) reporting and sharing, for an agency operating or exercising control of a national security system, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for national security systems issued as directed by the President; and

''(F) reporting and sharing, for those agencies operating or exercising control of non-national security systems, information about information security incidents, cyber threat information, and deterioration of security controls to the individual or entity designated at each cybersecurity center and to other appropriate entities consistent with policies and directives for non-national security systems as prescribed under section 3553(a), including information to assist the entity designated under section 3555(a) with the ongoing security analysis under section 3555;

''(2) ensure that each senior agency official provides information security for the information and information systems that support the operations and assets under the senior agency official's control, including by—

''(A) assessing the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

''(B) determining the level of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3553(a), and standards and guidelines promulgated under section 11331 of title 40 for information security classifications and related requirements;

''(C) implementing policies, procedures, and capabilities to reduce risks to an acceptable level in a cost-effective manner;

''(D) actively monitoring the effective implementation of information security controls and techniques; and

''(E) reporting information about information security incidents, cyber threat information, and deterioration of security controls in a timely and adequate manner to the entity designated under section 3553(a)(3) in accordance with paragraph (1);

''(3) assess and maintain the resiliency of information technology systems critical to agency mission and operations;

''(4) designate the agency Inspector General (or an independent entity selected in consultation with the Director and the Council of Inspectors General on Integrity and Efficiency if the agency does not have an Inspector General) to conduct the annual independent evaluation required under section 3556, and allow the agency Inspector General to contract with an independent entity to perform such evaluation;

''(5) delegate to the Chief Information Officer or equivalent (or to a senior agency official who reports to the Chief Information Officer or equivalent)—

''(A) the authority and primary responsibility to implement an agencywide information security program; and

''(B) the authority to provide information security for the information collected and maintained by the agency (or by a contractor, other agency, or other source on behalf of the agency) and for the information systems that support the operations, assets, and mission of the agency (including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency);

''(6) delegate to the appropriate agency official (who is responsible for a particular agency system or subsystem) the responsibility to ensure and enforce compliance with all requirements of the agency's agencywide information security program in coordination with the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5);

''(7) ensure that an agency has trained personnel who have obtained any necessary security clearances to permit them to assist the agency in complying with this subchapter;

''(8) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5), in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agencywide information security program, including the progress of any remedial actions; and

''(9) ensure that the Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under paragraph (5) has the necessary qualifications to administer the functions described in this subchapter and has information security duties as a primary duty of that official.

''(b) CHIEF INFORMATION OFFICERS.—Each Chief Information Officer or equivalent (or the senior agency official who reports to the Chief Information Officer or equivalent) under subsection (a)(5) shall—

''(1) establish and maintain an enterprise security operations capability that on a continuous basis—

''(A) detects, reports, contains, mitigates, and responds to information security incidents that impair adequate security of the agency's information or information system in a timely manner and in accordance with the policies and directives under section 3553; and

''(B) reports any information security incident under subparagraph (A) to the entity designated under section 3555;

''(2) develop, maintain, and oversee an agencywide information security program;

''(3) develop, maintain, and oversee information security policies, procedures, and control techniques to address applicable requirements, including requirements under section 3553 of this title and section 11331 of title 40; and

''(4) train and oversee the agency personnel who have significant responsibility for information security with respect to that responsibility.

''(c) AGENCYWIDE INFORMATION SECURITY PROGRAMS.—

''(1) IN GENERAL.—Each agencywide information security program under subsection (b)(2) shall include—

''(A) relevant security risk assessments, including technical assessments and others related to the acquisition process;

''(B) security testing commensurate with risk and impact;

''(C) mitigation of deterioration of security controls commensurate with risk and impact;

''(D) risk-based continuous monitoring and threat assessment of the operational status and security of agency information systems to enable evaluation of the effectiveness of and compliance with information security policies, procedures, and practices, including a relevant and appropriate selection of security controls of information systems identified in the inventory under section 3505(c);

''(E) operation of appropriate technical capabilities in order to detect, mitigate, report, and respond to information security incidents, cyber threat information, and deterioration of security controls in a manner that is consistent with the policies and directives under section 3553, including—

''(i) mitigating risks associated with such information security incidents;

''(ii) notifying and consulting with the entity designated under section 3555; and

''(iii) notifying and consulting with, as appropriate—

''(I) law enforcement and the relevant Office of the Inspector General; and

''(II) any other entity, in accordance with law and as directed by the President;

''(F) a process to ensure that remedial action is taken to address any deficiencies in the information security policies, procedures, and practices of the agency; and

''(G) a plan and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency.

''(2) RISK MANAGEMENT STRATEGIES.—Each agencywide information security program under subsection (b)(2) shall include the development and maintenance of a risk management strategy for information security. The risk management strategy shall include—

''(A) consideration of information security incidents, cyber threat information, and deterioration of security controls; and

''(B) consideration of the consequences that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, including any information system provided or managed by a contractor, other agency, or other source on behalf of the agency;

''(3) POLICIES AND PROCEDURES.—Each agencywide information security program under subsection (b)(2) shall include policies and procedures that—

''(A) are based on the risk management strategy under paragraph (2);

''(B) reduce information security risks to an acceptable level in a cost-effective manner;

''(C) ensure that cost-effective and adequate information security is addressed as part of the acquisition and ongoing management of each agency information system; and

''(D) ensure compliance with—

''(i) this subchapter; and

''(ii) any other applicable requirements.

''(4) TRAINING REQUIREMENTS.—Each agencywide information security program under subsection (b)(2) shall include information security, privacy, civil rights, civil liberties, and information oversight training that meets any applicable requirements under section 3553. The training shall inform each information security personnel that has access to agency information systems (including contractors and other users of information systems that support the operations and assets of the agency) of—

''(A) the information security risks associated with the information security personnel's activities; and

''(B) the individual's responsibility to comply with the agency policies and procedures that reduce the risks under subparagraph (A).

''(d) ANNUAL REPORT.—Each agency shall submit a report annually to the Secretary of Homeland Security on its agencywide information security program and information systems.

''§ 3555. Multiagency ongoing threat assessment

''(a) IMPLEMENTATION.—The Director of the Office of Management and Budget, in coordination with the Secretary of Homeland Security, shall designate an entity to implement ongoing security analysis concerning agency information systems—

''(1) based on cyber threat information;

''(2) based on agency information system and environment of operation changes, including—

''(A) an ongoing evaluation of the information system security controls; and

''(B) the security state, risk level, and environment of operation of an agency information system, including—

''(i) a change in risk level due to a new cyber threat;

''(ii) a change resulting from a new technology;

''(iii) a change resulting from the agency's mission; and

''(iv) a change resulting from the business practice; and

''(3) using automated processes to the maximum extent possible—

''(A) to increase information system security;

''(B) to reduce paper-based reporting requirements; and

''(C) to maintain timely and actionable knowledge of the state of the information system security.

''(b) STANDARDS.—The National Institute of Standards and Technology may promulgate standards, in coordination with the Secretary of Homeland Security, to assist an agency with its duties under this section.

''(c) COMPLIANCE.—The head of each appropriate department and agency shall be responsible for ensuring compliance and implementing necessary procedures to comply with this section. The head of each appropriate department and agency, in consultation with the Director of the Office of Management and Budget and the Secretary of Homeland Security, shall—

''(1) monitor compliance under this section;

''(2) develop a timeline and implement for the department or agency—

''(A) adoption of any technology, system, or method that facilitates continuous monitoring and threat assessments of an agency information system;

''(B) adoption or updating of any technology, system, or method that prevents, detects, or remediates a significant cyber incident to a Federal information system of the department or agency that has impeded, or is reasonably likely to impede, the performance of a critical mission of the department or agency; and

''(C) adoption of any technology, system, or method that satisfies a requirement under this section.

''(d) LIMITATION OF AUTHORITY.—The authorities of the Director of the Office of Management and Budget and of the Secretary of Homeland Security under this section shall not apply to national security systems.

''(e) REPORT.—Not later than 6 months after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Government Accountability Office shall issue a report evaluating each agency's status toward implementing this section.

''§ 3556. Independent evaluations

''(a) IN GENERAL.—The Council of the Inspectors General on Integrity and Efficiency, in consultation with the Director and the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense, shall issue and maintain criteria for the timely, cost-effective, risk-based, and independent evaluation of each agencywide information security program (and practices) to determine the effectiveness of the agencywide information security program (and practices). The criteria shall include measures to assess any conflicts of interest in the performance of the evaluation and whether the agencywide information security program includes appropriate safeguards against disclosure of information where such disclosure may adversely affect information security.

''(b) ANNUAL INDEPENDENT EVALUATIONS.—Each agency shall perform an annual independent evaluation of its agencywide information security program (and practices) in accordance with the criteria under subsection (a).

''(c) DISTRIBUTION OF REPORTS.—Not later than 30 days after receiving an independent evaluation under subsection (b), each agency head shall transmit a copy of the independent evaluation to the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense.

''(d) NATIONAL SECURITY SYSTEMS.—Evaluations involving national security systems shall be conducted as directed by President.

''§ 3557. National security systems.

''The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

''(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system; and

''(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President.''.

(b) SAVINGS PROVISIONS.—

(1) POLICY AND COMPLIANCE GUIDANCE.—Policy and compliance guidance issued by the Director before the date of enactment of this Act under section 3543(a)(1) of title 44, United States Code (as in effect on the day before the date of enactment of this Act), shall continue in effect, according to its terms, until modified, terminated, superseded, or repealed pursuant to section 3553(a)(1) of title 44, United States Code.

(2) STANDARDS AND GUIDELINES.—Standards and guidelines issued by the Secretary of Commerce or by the Director before the date of enactment of this Act under section 11331(a)(1) of title 40, United States Code, (as in effect on the day before the date of enactment of this Act) shall continue in effect, according to their terms, until modified, terminated, superseded, or repealed pursuant to section 11331(a)(1) of title 40, United States Code, as amended by this Act.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) CHAPTER ANALYSIS.—The chapter analysis for chapter 35 of title 44, United States Code, is amended—

(A) by striking the items relating to sections 3531 through 3538;

(B) by striking the items relating to sections 3541 through 3549; and

(C) by inserting the following:

''3551. Purposes.
''3552. Definitions.
''3553. Federal information security authority and coordination.
''3554. Agency responsibilities.
''3555. Multiagency ongoing threat assessment.
''3556. Independent evaluations.
''3557. National security systems.''.

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3532(3)'' and inserting ''section 3552''.

(B) Section 2222(j)(5) of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(C) Section 2223(c)(3) of title 10, United States Code, is amended, by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(D) Section 2315 of title 10, United States Code, is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552''.

(E) Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3532(b)(2)'' and inserting ''section 3552'';

(ii) in subsection (c)(3), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iii) in subsection (d)(1), by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(iv) in subsection (d)(8) by striking ''Director of the Office of Management and Budget'' and inserting ''Secretary of Commerce'';

(v) in subsection (d)(8), by striking ''submitted to the Director'' and inserting ''submitted to the Secretary'';

(vi) in subsection (e)(2), by striking ''section 3532(1) of such title'' and inserting ''section 3552 of title 44''; and

(vii) in subsection (e)(5), by striking ''section 3532(b)(2) of such title'' and inserting ''section 3552 of title 44''.

(F) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking ''section 3534(b)'' and inserting ''section 3554(b)(2)''.

SEC. 202. MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) IN GENERAL.—Section 11331 of title 40, United States Code, is amended to read as follows:

''§ 11331. Responsibilities for Federal information systems standards

''(a) STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO PRESCRIBE.—Except as provided under paragraph (2), the Secretary of Commerce shall prescribe standards and guidelines pertaining to Federal information systems—

''(A) in consultation with the Secretary of Homeland Security; and

''(B) on the basis of standards and guidelines developed by the National Institute of Standards and Technology under paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)(2) and (a)(3)).

''(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.

''(b) MANDATORY STANDARDS AND GUIDELINES.—

''(1) AUTHORITY TO MAKE MANDATORY STANDARDS AND GUIDELINES.—The Secretary of Commerce shall make standards and guidelines under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of Federal information systems.

''(2) REQUIRED MANDATORY STANDARDS AND GUIDELINES.—

''(A) IN GENERAL.—Standards and guidelines under subsection (a)(1) shall include information security standards that—

''(i) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

''(ii) are otherwise necessary to improve the security of Federal information and information systems.

''(B) BINDING EFFECT.—Information security standards under subparagraph (A) shall be compulsory and binding.

''(c) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary of Commerce shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director.

''(d) APPLICATION OF MORE STRINGENT STANDARDS AND GUIDELINES.—The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards and guidelines the Secretary of Commerce prescribes under this section if the more stringent standards and guidelines—

''(1) contain at least the applicable standards and guidelines made compulsory and binding by the Secretary of Commerce; and

''(2) are otherwise consistent with the policies, directives, and implementation memoranda issued under section 3553(a) of title 44.

''(e) DECISIONS ON PROMULGATION OF STANDARDS AND GUIDELINES.—The decision by the Secretary of Commerce regarding the promulgation of any standard or guideline under this section shall occur not later than 6 months after the date of submission of the proposed standard to the Secretary of Commerce by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

''(f) NOTICE AND COMMENT.—A decision by the Secretary of Commerce to significantly modify, or not promulgate, a proposed standard submitted to the Secretary by the National Institute of Standards and Technology under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) shall be made after the public is given an opportunity to comment on the Secretary's proposed decision.

''(g) DEFINITIONS.—In this section:

''(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' has the meaning given the term in section 3552 of title 44.

''(2) INFORMATION SECURITY.—The term 'information security' has the meaning given the term in section 3552 of title 44.

''(3) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 3552 of title 44.''.

SEC. 203. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

SEC. 204. TECHNICAL AND CONFORMING AMENDMENTS.

Section 21(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4(b)) is amended—

(1) in paragraph (2), by striking ''and the Director of the Office of Management and Budget'' and inserting '', the Secretary of Commerce, and the Secretary of Homeland Security''; and

(2) in paragraph (3), by inserting '', the Secretary of Homeland Security,'' after ''the Secretary of Commerce''.

SEC. 205. CLARIFICATION OF AUTHORITIES.

Nothing in this title shall be construed to convey any new regulatory authority to any government entity implementing or complying with any provision of this title.

TITLE III—CRIMINAL PENALTIES

SEC. 301. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended to read as follows:

''(c) The punishment for an offense under subsection (a) or (b) of this section is—

''(1) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(1) of this section;

''(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than 3 years, or both, in the case of an offense under subsection (a)(2); or

''(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2) of this section, if—

''(i) the offense was committed for purposes of commercial advantage or private financial gain;

''(ii) the offense was committed in the furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States, or of any State; or

''(iii) the value of the information obtained, or that would have been obtained if the offense was completed, exceeds $5,000;

''(3) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(3) of this section;

''(4) a fine under this title or imprisonment of not more than 20 years, or both, in the case of an offense under subsection (a)(4) of this section;

''(5)(A) except as provided in subparagraph (C), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A) of this section, if the offense caused—

''(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

''(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

''(iii) physical injury to any person;

''(iv) a threat to public health or safety;

''(v) damage affecting a computer used by, or on behalf of, an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

''(vi) damage affecting 10 or more protected computers during any 1-year period;

''(B) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(B), if the offense caused a harm provided in clause (i) through (vi) of subparagraph (A) of this subsection;

''(C) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both;

''(D) a fine under this title, imprisonment for not more than 10 years, or both, for any other offense under subsection (a)(5);

''(E) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(6) of this section; or

''(F) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(7) of this section.''.

SEC. 302. TRAFFICKING IN PASSWORDS.

Section 1030(a)(6) of title 18, United States Code, is amended to read as follows:

''(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information or means of access through which a protected computer (as defined in subparagraphs (A) and (B) of subsection (e)(2)) may be accessed without authorization.''.

SEC. 303. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD OFFENSES.

Section 1030(b) of title 18, United States Code, is amended by inserting ''as if for the completed offense'' after ''punished as provided''.

SEC. 304. CRIMINAL AND CIVIL FORFEITURE FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended by striking subsections (i) and (j) and inserting the following:

''(i) CRIMINAL FORFEITURE.—

''(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

''(A) such persons interest in any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

''(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

''(2) The criminal forfeiture of property under this subsection, including any seizure

and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

''(j) CIVIL FORFEITURE.—

''(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them:

''(A) Any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

''(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

''(2) Seizures and forfeitures under this subsection shall be governed by the provisions in chapter 46 relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) shall be performed by such officers, agents and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.''.

SEC. 305. DAMAGE TO CRITICAL INFRASTRUCTURE COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) DEFINITIONS.—In this section—

''(1) the term 'computer' has the meaning given the term in section 1030;

''(2) the term 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated, including—

''(A) oil and gas production, storage, conversion, and delivery systems;

''(B) water supply systems;

''(C) telecommunication networks;

''(D) electrical power generation and delivery systems;

''(E) finance and banking systems;

''(F) emergency services;

''(G) transportation systems and services; and

''(H) government operations that provide essential services to the public; and

''(3) the term 'damage' has the meaning given the term in section 1030.

''(b) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer if the damage results in (or, in the case of an attempt, if completed, would have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with the computer.

''(c) PENALTY.—Any person who violates subsection (b) shall be—

''(1) fined under this title;

''(2) imprisoned for not less than 3 years but not more than 20 years; or

''(3) penalized under paragraphs (1) and (2).

''(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place on probation any person convicted of a violation of this section;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for a felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The chapter analysis for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. 306. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.

Section 1030(e)(6) of title 18, United States Code, is amended by striking ''alter;'' and inserting ''alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;''.

SEC. 307. NO NEW FUNDING.

An applicable Federal agency shall carry out the provisions of this title with existing facilities and funds otherwise available, through such means as the head of the agency considers appropriate.

TITLE IV—CYBERSECURITY RESEARCH AND DEVELOPMENT

SEC. 401. NATIONAL HIGH-PERFORMANCE COMPUTING PROGRAM PLANNING AND COORDINATION.

(a) GOALS AND PRIORITIES.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(d) GOALS AND PRIORITIES.—The goals and priorities for Federal high-performance computing research, development, networking, and other activities under subsection (a)(2)(A) shall include—

''(1) encouraging and supporting mechanisms for interdisciplinary research and development in networking and information technology, including—

''(A) through collaborations across agencies;

''(B) through collaborations across Program Component Areas;

''(C) through collaborations with industry;

''(D) through collaborations with institutions of higher education;

''(E) through collaborations with Federal laboratories (as defined in section 4 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3703)); and

''(F) through collaborations with international organizations;

''(2) addressing national, multi-agency, multi-faceted challenges of national importance; and

''(3) fostering the transfer of research and development results into new technologies and applications for the benefit of society.''.

(b) DEVELOPMENT OF STRATEGIC PLAN.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(e) STRATEGIC PLAN.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the agencies under subsection (a)(3)(B), working through the National Science and Technology Council and with the assistance of the Office of Science and Technology Policy shall develop a 5-year strategic plan to guide the activities under subsection (a)(1).

''(2) CONTENTS.—The strategic plan shall specify—

''(A) the near-term objectives for the Program;

''(B) the long-term objectives for the Program;

''(C) the anticipated time frame for achieving the near-term objectives;

''(D) the metrics that will be used to assess any progress made toward achieving the near-term objectives and the long-term objectives; and

''(E) how the Program will achieve the goals and priorities under subsection (d).

''(3) IMPLEMENTATION ROADMAP.—

''(A) IN GENERAL.—The agencies under subsection (a)(3)(B) shall develop and annually update an implementation roadmap for the strategic plan.

''(B) REQUIREMENTS.—The information in the implementation roadmap shall be coordinated with the database under section 102(c) and the annual report under section 101(a)(3). The implementation roadmap shall—

''(i) specify the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated, with consideration of any relevant recommendations of the advisory committee;

''(ii) specify the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year; and

''(iii) estimate the funding required for each major research objective of the strategic plan for the next 3 fiscal years.

''(4) RECOMMENDATIONS.—The agencies under subsection (a)(3)(B) shall take into consideration when developing the strategic plan under paragraph (1) the recommendations of—

''(A) the advisory committee under subsection (b); and

''(B) the stakeholders under section 102(a)(3).

''(5) REPORT TO CONGRESS.—The Director of the Office of Science and Technology Policy shall transmit the strategic plan under this subsection, including the implementation roadmap and any updates under paragraph (3), to—

''(A) the advisory committee under subsection (b);

''(B) the Committee on Commerce, Science, and Transportation of the Senate; and

''(C) the Committee on Science and Technology of the House of Representatives.''.

(c) PERIODIC REVIEWS.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended by adding at the end the following:

''(f) PERIODIC REVIEWS.—The agencies under subsection (a)(3)(B) shall—

''(1) periodically assess the contents and funding levels of the Program Component

Areas and restructure the Program when warranted, taking into consideration any relevant recommendations of the advisory committee under subsection (b); and

''(2) ensure that the Program includes national, multi-agency, multi-faceted research and development activities, including activities described in section 104.''.

(d) ADDITIONAL RESPONSIBILITIES OF DIRECTOR.—Section 101(a)(2) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(2)) is amended—

(1) by redesignating subparagraphs (E) and (F) as subparagraphs (G) and (H), respectively; and

(2) by inserting after subparagraph (D) the following:

''(E) encourage and monitor the efforts of the agencies participating in the Program to allocate the level of resources and management attention necessary—

''(i) to ensure that the strategic plan under subsection (e) is developed and executed effectively; and

''(ii) to ensure that the objectives of the Program are met;

''(F) working with the Office of Management and Budget and in coordination with the creation of the database under section 102(c), direct the Office of Science and Technology Policy and the agencies participating in the Program to establish a mechanism (consistent with existing law) to track all ongoing and completed research and development projects and associated funding;''.

(e) ADVISORY COMMITTEE.—Section 101(b) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(b)) is amended—

(1) in paragraph (1)—

(A) by inserting after the first sentence the following: ''The co-chairs of the advisory committee shall meet the qualifications of committee members and may be members of the Presidents Council of Advisors on Science and Technology.''; and

(B) by striking ''high-performance'' in subparagraph (D) and inserting ''high-end''; and

(2) by amending paragraph (2) to read as follows:

''(2) In addition to the duties under paragraph (1), the advisory committee shall conduct periodic evaluations of the funding, management, coordination, implementation, and activities of the Program. The advisory committee shall report its findings and recommendations not less frequently than once every 3 fiscal years to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives. The report shall be submitted in conjunction with the update of the strategic plan.''.

(f) REPORT.—Section 101(a)(3) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(3)) is amended—

(1) in subparagraph (C)—

(A) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(B) by striking ''each Program Component Area'' and inserting ''each Program Component Area and each research area supported in accordance with section 104'';

(2) in subparagraph (D)—

(A) by striking ''each Program Component Area,'' and inserting ''each Program Component Area and each research area supported in accordance with section 104,'';

(B) by striking ''is submitted,'' and inserting ''is submitted, the levels for the previous fiscal year,''; and

(C) by striking ''and'' after the semicolon;

(3) by redesignating subparagraph (E) as subparagraph (G); and

(4) by inserting after subparagraph (D) the following:

''(E) include a description of how the objectives for each Program Component Area, and the objectives for activities that involve multiple Program Component Areas, relate to the objectives of the Program identified in the strategic plan under subsection (e);

''(F) include—

''(i) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the next fiscal year by category of activity;

''(ii) a description of the funding required by the Office of Science and Technology Policy to perform the functions under subsections (a) and (c) of section 102 for the current fiscal year by category of activity; and

''(iii) the amount of funding provided for the Office of Science and Technology Policy for the current fiscal year by each agency participating in the Program; and''.

(g) DEFINITIONS.—Section 4 of the High-Performance Computing Act of 1991 (15 U.S.C. 5503) is amended—

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

(2) by redesignating paragraph (3) as paragraph (6);

(3) by redesignating paragraphs (6) and (7) as paragraphs (7) and (8), respectively;

(4) by inserting before paragraph (2), as redesignated, the following:

''(1) 'cyber-physical systems' means physical or engineered systems whose networking and information technology functions and physical elements are deeply integrated and are actively connected to the physical world through sensors, actuators, or other means to perform monitoring and control functions;'';

(5) in paragraph (3), as redesignated, by striking ''high-performance computing'' and inserting ''networking and information technology'';

(6) in paragraph (6), as redesignated—

(A) by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(B) by striking ''supercomputer'' and inserting ''high-end computing'';

(7) in paragraph (5), by striking ''network referred to as'' and all that follows through the semicolon and inserting ''network, including advanced computer networks of Federal agencies and departments''; and

(8) in paragraph (7), as redesignated, by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program''.

SEC. 402. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

(a) RESEARCH IN AREAS OF NATIONAL IMPORTANCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.) is amended by adding at the end the following:

''SEC. 104. RESEARCH IN AREAS OF NATIONAL IMPORTANCE.

''(a) IN GENERAL.—The Program shall encourage agencies under section 101(a)(3)(B) to support, maintain, and improve national, multi-agency, multi-faceted, research and development activities in networking and information technology directed toward application areas that have the potential for significant contributions to national economic competitiveness and for other significant societal benefits.

''(b) TECHNICAL SOLUTIONS.—An activity under subsection (a) shall be designed to advance the development of research discoveries by demonstrating technical solutions to important problems in areas including—

''(1) cybersecurity;

''(2) health care;

''(3) energy management and low-power systems and devices;

''(4) transportation, including surface and air transportation;

''(5) cyber-physical systems;

''(6) large-scale data analysis and modeling of physical phenomena;

''(7) large scale data analysis and modeling of behavioral phenomena;

''(8) supply chain quality and security; and

''(9) privacy protection and protected disclosure of confidential data.

''(c) RECOMMENDATIONS.—The advisory committee under section 101(b) shall make recommendations to the Program for candidate research and development areas for support under this section.

''(d) CHARACTERISTICS.—

''(1) IN GENERAL.—Research and development activities under this section—

''(A) shall include projects selected on the basis of applications for support through a competitive, merit-based process;

''(B) shall leverage, when possible, Federal investments through collaboration with related State initiatives;

''(C) shall include a plan for fostering the transfer of research discoveries and the results of technology demonstration activities, including from institutions of higher education and Federal laboratories, to industry for commercial development;

''(D) shall involve collaborations among researchers in institutions of higher education and industry; and

''(E) may involve collaborations among nonprofit research institutions and Federal laboratories, as appropriate.

''(2) COST-SHARING.—In selecting applications for support, the agencies under section 101(a)(3)(B) shall give special consideration to projects that include cost sharing from non-Federal sources.

''(3) MULTIDISCIPLINARY RESEARCH CENTERS.—Research and development activities under this section shall be supported through multidisciplinary research centers, including Federal laboratories, that are organized to investigate basic research questions and carry out technology demonstration activities in areas described in subsection (a). Research may be carried out through existing multidisciplinary centers, including those authorized under section 7024(b)(2) of the America COMPETES Act (42 U.S.C. 1862o–10(2)).''.

(b) CYBER-PHYSICAL SYSTEMS.—Section 101(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5511(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

''(J) provide for increased understanding of the scientific principles of cyber-physical systems and improve the methods available for the design, development, and operation of cyber-physical systems that are characterized by high reliability, safety, and security; and

''(K) provide for research and development on human-computer interactions, visualization, and big data.''.

(c) TASK FORCE.—Title I of the High-Performance Computing Act of 1991 (15 U.S.C. 5511 et seq.), as amended by section 402(a) of this Act, is amended by adding at the end the following:

''SEC. 105. TASK FORCE.

''(a) ESTABLISHMENT.—Not later than 180 days after the date of enactment the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy under section 102 shall convene a task force

to explore mechanisms for carrying out collaborative research and development activities for cyber-physical systems (including the related technologies required to enable these systems) through a consortium or other appropriate entity with participants from institutions of higher education, Federal laboratories, and industry.

''(b) FUNCTIONS.—The task force shall—

''(1) develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activities;

''(2) propose a process for developing a research and development agenda for such entity, including guidelines to ensure an appropriate scope of work focused on nationally significant challenges and requiring collaboration and to ensure the development of related scientific and technological milestones;

''(3) define the roles and responsibilities for the participants from institutions of higher education, Federal laboratories, and industry in such entity;

''(4) propose guidelines for assigning intellectual property rights and for transferring research results to the private sector; and

''(5) make recommendations for how such entity could be funded from Federal, State, and non-governmental sources.

''(c) COMPOSITION.—In establishing the task force under subsection (a), the Director of the Office of Science and Technology Policy shall appoint an equal number of individuals from institutions of higher education and from industry with knowledge and expertise in cyber-physical systems, and may appoint not more than 2 individuals from Federal laboratories.

''(d) REPORT.—Not later than 1 year after the date of enactment of the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, the Director of the Office of Science and Technology Policy shall transmit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science and Technology of the House of Representatives a report describing the findings and recommendations of the task force.

''(e) TERMINATION.—The task force shall terminate upon transmittal of the report required under subsection (d).

''(f) COMPENSATION AND EXPENSES.—Members of the task force shall serve without compensation.''.

SEC. 403. PROGRAM IMPROVEMENTS.

Section 102 of the High-Performance Computing Act of 1991 (15 U.S.C. 5512) is amended to read as follows:

''SEC. 102. PROGRAM IMPROVEMENTS.

''(a) FUNCTIONS.—The Director of the Office of Science and Technology Policy shall continue—

''(1) to provide technical and administrative support to—

''(A) the agencies participating in planning and implementing the Program, including support needed to develop the strategic plan under section 101(e); and

''(B) the advisory committee under section 101(b);

''(2) to serve as the primary point of contact on Federal networking and information technology activities for government agencies, academia, industry, professional societies, State computing and networking technology programs, interested citizen groups, and others to exchange technical and programmatic information;

''(3) to solicit input and recommendations from a wide range of stakeholders during the development of each strategic plan under section 101(e) by convening at least 1 workshop with invitees from academia, industry, Federal laboratories, and other relevant organizations and institutions;

''(4) to conduct public outreach, including the dissemination of the advisory committee's findings and recommendations, as appropriate;

''(5) to promote access to and early application of the technologies, innovations, and expertise derived from Program activities to agency missions and systems across the Federal Government and to United States industry;

''(6) to ensure accurate and detailed budget reporting of networking and information technology research and development investment; and

''(7) to encourage agencies participating in the Program to use existing programs and resources to strengthen networking and information technology education and training, and increase participation in such fields, including by women and underrepresented minorities.

''(b) SOURCE OF FUNDING.—

''(1) IN GENERAL.—The functions under this section shall be supported by funds from each agency participating in the Program.

''(2) SPECIFICATIONS.—The portion of the total budget of the Office of Science and Technology Policy that is provided by each agency participating in the Program for each fiscal year shall be in the same proportion as each agency's share of the total budget for the Program for the previous fiscal year, as specified in the database under section 102(c).

''(c) DATABASE.—

''(1) IN GENERAL.—The Director of the Office of Science and Technology Policy shall develop and maintain a database of projects funded by each agency for the fiscal year for each Program Component Area.

''(2) PUBLIC ACCESSIBILITY.—The Director of the Office of Science and Technology Policy shall make the database accessible to the public.

''(3) DATABASE CONTENTS.—The database shall include, for each project in the database—

''(A) a description of the project;

''(B) each agency, industry, institution of higher education, Federal laboratory, or international institution involved in the project;

''(C) the source funding of the project (set forth by agency);

''(D) the funding history of the project; and

''(E) whether the project has been completed.''.

SEC. 404. IMPROVING EDUCATION OF NETWORKING AND INFORMATION TECHNOLOGY, INCLUDING HIGH PERFORMANCE COMPUTING.

Section 201(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)) is amended—

(1) by redesignating paragraphs (2) through (4) as paragraphs (3) through (5), respectively; and

(2) by inserting after paragraph (1) the following:

''(2) the National Science Foundation shall use its existing programs, in collaboration with other agencies, as appropriate, to improve the teaching and learning of networking and information technology at all levels of education and to increase participation in networking and information technology fields;''.

SEC. 405. CONFORMING AND TECHNICAL AMENDMENTS TO THE HIGH-PERFORMANCE COMPUTING ACT OF 1991.

(a) SECTION 3.—Section 3 of the High-Performance Computing Act of 1991 (15 U.S.C. 5502) is amended—

(1) in the matter preceding paragraph (1), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(2) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking ''high-performance computing'' and inserting ''networking and information technology'';

(B) in subparagraphs (A), (F), and (G), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(C) in subparagraph (H), by striking ''high-performance'' and inserting ''high-end''; and

(3) in paragraph (2)—

(A) by striking ''high-performance computing and'' and inserting ''networking and information technology, and''; and

(B) by striking ''high-performance computing network'' and inserting ''networking and information technology''.

(b) TITLE HEADING.—The heading of title I of the High-Performance Computing Act of 1991 (105 Stat. 1595) is amended by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''.

(c) SECTION 101.—Section 101 of the High-Performance Computing Act of 1991 (15 U.S.C. 5511) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT**'';

(2) in subsection (a)—

(A) in the subsection heading, by striking ''NATIONAL HIGH-PERFORMANCE COMPUTING'' and inserting ''NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT'';

(B) in paragraph (1)—

(i) by striking ''National High-Performance Computing Program'' and inserting ''networking and information technology research and development program'';

(ii) in subparagraph (A), by striking ''high-performance computing, including networking'' and inserting ''networking and information technology'';

(iii) in subparagraphs (B) and (G), by striking ''high-performance'' each place it appears and inserting ''high-end''; and

(iv) in subparagraph (C), by striking ''high-performance computing and networking'' and inserting ''high-end computing, distributed, and networking''; and

(C) in paragraph (2)—

(i) in subparagraphs (A) and (C)—

(I) by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(II) by striking ''development, networking,'' each place it appears and inserting ''development,''; and

(ii) in subparagraphs (G) and (H), as redesignated by section 401(d) of this Act, by striking ''high-performance'' each place it appears and inserting ''high-end'';

(3) in subsection (b)(1), in the matter preceding subparagraph (A), by striking ''high-performance computing'' each place it appears and inserting ''networking and information technology''; and

(4) in subsection (c)(1)(A), by striking ''high-performance computing'' and inserting ''networking and information technology''.

(d) SECTION 201.—Section 201(a)(1) of the High-Performance Computing Act of 1991 (15 U.S.C. 5521(a)(1)) is amended by striking ''high-performance computing and advanced high-speed computer networking'' and inserting ''networking and information technology research and development''.

(e) SECTION 202.—Section 202(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5522(a)) is amended by striking ''high-

performance computing'' and inserting ''networking and information technology''.

(f) SECTION 203.—Section 203(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5523(a)) is amended—

(1) in paragraph (1), by striking ''high-performance computing and networking'' and inserting ''networking and information technology''; and

(2) in paragraph (2)(A), by striking ''high-performance'' and inserting ''high-end''.

(g) SECTION 204.—Section 204 of the High-Performance Computing Act of 1991 (15 U.S.C. 5524) is amended—

(1) in subsection (a)(1)—

(A) in subparagraph (A), by striking ''high-performance computing systems and networks'' and inserting ''networking and information technology systems and capabilities'';

(B) in subparagraph (B), by striking ''interoperability of high-performance computing systems in networks and for common user interfaces to systems'' and inserting ''interoperability and usability of networking and information technology systems''; and

(C) in subparagraph (C), by striking ''high-performance computing'' and inserting ''networking and information technology''; and

(2) in subsection (b)—

(A) by striking ''HIGH-PERFORMANCE COMPUTING AND NETWORK'' in the heading and inserting ''NETWORKING AND INFORMATION TECHNOLOGY''; and

(B) by striking ''sensitive''.

(h) SECTION 205.—Section 205(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5525(a)) is amended by striking ''computational'' and inserting ''networking and information technology''.

(i) SECTION 206.—Section 206(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5526(a)) is amended by striking ''computational research'' and inserting ''networking and information technology research''.

(j) SECTION 207.—Section 207 of the High-Performance Computing Act of 1991 (15 U.S.C. 5527) is amended by striking ''high-performance computing'' and inserting ''networking and information technology''.

(k) SECTION 208.—Section 208 of the High-Performance Computing Act of 1991 (15 U.S.C. 5528) is amended—

(1) in the section heading, by striking ''**HIGH-PERFORMANCE COMPUTING**'' and inserting ''**NETWORKING AND INFORMATION TECHNOLOGY**''; and

(2) in subsection (a)—

(A) in paragraph (1), by striking ''High-performance computing and associated'' and inserting ''Networking and information'';

(B) in paragraph (2), by striking ''high-performance computing'' and inserting ''networking and information technologies'';

(C) in paragraph (3), by striking ''high-performance'' and inserting ''high-end'';

(D) in paragraph (4), by striking ''high-performance computers and associated'' and inserting ''networking and information''; and

(E) in paragraph (5), by striking ''high-performance computing and associated'' and inserting ''networking and information''.

SEC. 406. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with the Secretary of Homeland Security, shall carry out a Federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals and security managers to meet the needs of the cybersecurity mission for the Federal government.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The program shall—

(1) annually assess the workforce needs of the Federal government for cybersecurity professionals, including network engineers, software engineers, and other experts in order to determine how many scholarships should be awarded annually to ensure that the workforce needs following graduation match the number of scholarships awarded;

(2) provide scholarships for up to 1,000 students per year in their pursuit of undergraduate or graduate degrees in the cybersecurity field, in an amount that may include coverage for full tuition, fees, and a stipend;

(3) require each scholarship recipient, as a condition of receiving a scholarship under the program, to serve in a Federal information technology workforce for a period equal to one and one-half times each year, or partial year, of scholarship received, in addition to an internship in the cybersecurity field, if applicable, following graduation;

(4) provide a procedure for the National Science Foundation or a Federal agency, consistent with regulations of the Office of Personnel Management, to request and fund a security clearance for a scholarship recipient, including providing for clearance during a summer internship and upon graduation; and

(5) provide opportunities for students to receive temporary appointments for meaningful employment in the Federal information technology workforce during school vacation periods and for internships.

(c) HIRING AUTHORITY.—

(1) IN GENERAL.—For purposes of any law or regulation governing the appointment of an individual in the Federal civil service, upon the successful completion of the student's studies, a student receiving a scholarship under the program may—

(A) be hired under section 213.3102(r) of title 5, Code of Federal Regulations; and

(B) be exempt from competitive service.

(2) COMPETITIVE SERVICE.—Upon satisfactory fulfillment of the service term under paragraph (1), an individual may be converted to a competitive service position without competition if the individual meets the requirements for that position.

(d) ELIGIBILITY.—The eligibility requirements for a scholarship under this section shall include that a scholarship applicant—

(1) be a citizen of the United States;

(2) be eligible to be granted a security clearance;

(3) maintain a grade point average of 3.2 or above on a 4.0 scale for undergraduate study or a 3.5 or above on a 4.0 scale for post-graduate study;

(4) demonstrate a commitment to a career in improving the security of the information infrastructure; and

(5) has demonstrated a level of proficiency in math or computer sciences.

(e) FAILURE TO COMPLETE SERVICE OBLIGATION.—

(1) IN GENERAL.—A scholarship recipient under this section shall be liable to the United States under paragraph (2) if the scholarship recipient—

(A) fails to maintain an acceptable level of academic standing in the educational institution in which the individual is enrolled, as determined by the Director;

(B) is dismissed from such educational institution for disciplinary reasons;

(C) withdraws from the program for which the award was made before the completion of such program;

(D) declares that the individual does not intend to fulfill the service obligation under this section;

(E) fails to fulfill the service obligation of the individual under this section; or

(F) loses a security clearance or becomes ineligible for a security clearance.

(2) REPAYMENT AMOUNTS.—

(A) LESS THAN 1 YEAR OF SERVICE.—If a circumstance under paragraph (1) occurs before the completion of 1 year of a service obligation under this section, the total amount of awards received by the individual under this section shall be repaid.

(B) ONE OR MORE YEARS OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of paragraph (1) occurs after the completion of 1 year of a service obligation under this section, the total amount of scholarship awards received by the individual under this section, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be repaid.

(f) EVALUATION AND REPORT.—The Director of the National Science Foundation shall—

(1) evaluate the success of recruiting individuals for scholarships under this section and of hiring and retaining those individuals in the public sector workforce, including the annual cost and an assessment of how the program actually improves the Federal workforce; and

(2) periodically report the findings under paragraph (1) to Congress.

(g) AUTHORIZATION OF APPROPRIATIONS.—From amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), the Director may use funds to carry out the requirements of this section for fiscal years 2012 through 2013.

SEC. 407. STUDY AND ANALYSIS OF CERTIFICATION AND TRAINING OF INFORMATION INFRASTRUCTURE PROFESSIONALS.

(a) STUDY.—The President shall enter into an agreement with the National Academies to conduct a comprehensive study of government, academic, and private-sector accreditation, training, and certification programs for personnel working in information infrastructure. The agreement shall require the National Academies to consult with sector coordinating councils and relevant governmental agencies, regulatory entities, and nongovernmental organizations in the course of the study.

(b) SCOPE.—The study shall include—

(1) an evaluation of the body of knowledge and various skills that specific categories of personnel working in information infrastructure should possess in order to secure information systems;

(2) an assessment of whether existing government, academic, and private-sector accreditation, training, and certification programs provide the body of knowledge and various skills described in paragraph (1);

(3) an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibility; and

(4) an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government and the private sector, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the National Academies shall submit to the President and Congress a report on the results of the study. The report shall include—

(1) findings regarding the state of information infrastructure accreditation, training, and certification programs, including specific areas of deficiency and demonstrable progress; and

(2) recommendations for the improvement of information infrastructure accreditation, training, and certification programs.

SEC. 408. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS.

(a) IN GENERAL.—The Director of the National Institute of Standards and Technology, in coordination with appropriate Federal authorities, shall—

(1) as appropriate, ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security; and

(2) not later than 1 year after the date of enactment of this Act, develop and transmit to Congress a plan for ensuring such Federal agency coordination.

(b) CONSULTATION WITH THE PRIVATE SECTOR.—In carrying out the activities under subsection (a)(1), the Director shall ensure consultation with appropriate private sector stakeholders.

SEC. 409. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT.

The Director of the National Institute of Standards and Technology shall continue a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns—

(1) to improve interoperability among identity management technologies;

(2) to strengthen authentication methods of identity management systems;

(3) to improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and

(4) to improve the usability of identity management systems.

SEC. 410. FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY RESEARCH GRANT AREAS.—Section 4(a)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(1)) is amended—

(1) in subparagraph (H), by striking ''and'' after the semicolon;

(2) in subparagraph (I), by striking ''property.'' and inserting ''property;''; and

(3) by adding at the end the following:

''(J) secure fundamental protocols that are at the heart of inter-network communications and data exchange;

''(K) system security that addresses the building of secure systems from trusted and untrusted components;

''(L) monitoring and detection; and

''(M) resiliency and rapid recovery methods.''.

(b) NATIONAL SCIENCE FOUNDATION COMPUTER AND NETWORK SECURITY GRANTS.—Section 4(a)(3) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)(3)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(c) COMPUTER AND NETWORK SECURITY CENTERS.—Section 4(b)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7403(b)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(d) COMPUTER AND NETWORK SECURITY CAPACITY BUILDING GRANTS.—Section 5(a)(6) of the Cyber Security Research and Development Act (15 U.S.C. 7404(a)(6)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(e) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT GRANTS.—Section 5(b)(2) of the Cyber Security Research and Development Act (15 U.S.C. 7404(b)(2)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

(f) GRADUATE TRAINEESHIPS IN COMPUTER AND NETWORK SECURITY RESEARCH.—Section 5(c)(7) of the Cyber Security Research and Development Act (15 U.S.C. 7404(c)(7)) is amended—

(1) in subparagraph (D), by striking ''and'';

(2) in subparagraph (E), by striking ''2007.'' and inserting ''2007;''; and

(3) by adding at the end the following:

''(F) such funds from amounts made available under section 503 of the America COMPETES Reauthorization Act of 2010 (124 Stat. 4005), as the Director finds necessary to carry out the requirements of this subsection for fiscal years 2012 through 2013.''.

SA 2697. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. SENSE OF SENATE ON APPOINTMENT BY THE ATTORNEY GENERAL OF AN OUTSIDE SPECIAL COUNSEL TO INVESTIGATE CERTAIN RECENT LEAKS OF APPARENTLY CLASSIFIED AND HIGHLY SENSITIVE INFORMATION ON UNITED STATES MILITARY AND INTELLIGENCE PLANS, PROGRAMS, AND OPERATIONS.

(a) FINDINGS.—The Senate makes the following findings:

(1) Over the past few weeks, several publications have been released that cite several highly sensitive United States military and intelligence counterterrorism plans, programs, and operations.

(2) These publications appear to be based in substantial part on unauthorized disclosures of classified information.

(3) The unauthorized disclosure of classified information is a felony under Federal law.

(4) The identity of the sources in these publications include senior administration officials, participants in these reported plans, programs, and operations, and current American officials who spoke anonymously about these reported plans, programs, and operations because they remain classified, parts of them are ongoing, or both.

(5) Such unauthorized disclosures may inhibit the ability of the United States to employ the same or similar plans, programs, or operations in the future; put at risk the national security of the United States and the safety of the men and women sworn to protect it; and dismay our allies.

(6) Under Federal law, the Attorney General may appoint an outside special counsel when an investigation or prosecution would present a conflict of interest or other extraordinary circumstances and when doing so would serve the public interest.

(7) Investigations of unauthorized disclosures of classified information are ordinarily conducted by the Federal Bureau of Investigation with assistance from prosecutors in the National Security Division of the Department of Justice.

(8) There is precedent for officials in the National Security Division of the Department of Justice to recuse itself from such investigations to avoid even the appearance of impropriety or undue influence, and it appears that there have been such recusals with respect to the investigation of at least one of these unauthorized disclosures.

(9) Such recusals are indicative of the serious complications already facing the Department of Justice in investigating these matters.

(10) The severity of the national security implications of these disclosures; the imperative for investigations of these disclosures to be conducted independently so as to avoid even the appearance of impropriety or undue influence; and the need to conduct these investigations expeditiously to ensure timely mitigation constitute extraordinary circumstances.

(11) For the foregoing reasons, the appointment of an outside special counsel would serve the public interest.

(b) SENSE OF SENATE.—It is the sense of the Senate that—

(1) the Attorney General should—

(A) delegate to an outside special counsel all of the authority of the Attorney General with respect to investigations by the Department of Justice of any and all unauthorized disclosures of classified and highly sensitive information related to various United States military and intelligence plans, programs, and operations reported in recent publications; and

(B) direct an outside special counsel to exercise that authority independently of the supervision or control of any officer of the Department of Justice;

(2) under such authority, the outside special counsel should investigate any and all unauthorized disclosures of classified and highly sensitive information on which such recent publications were based and, where appropriate, prosecute those responsible; and

(3) the President should assess—

(A) whether any such unauthorized disclosures of classified and highly sensitive information damaged the national security of the United States; and

(B) how such damage can be mitigated.

SA 2698. Mr. PORTMAN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE ___—RESPONSE TO CONGRESSIONAL INQUIRIES

SEC. ___1. RESPONSE TO CONGRESSIONAL INQUIRIES REGARDING PUBLIC RELATIONS SPENDING BY THE DEPARTMENT OF HEALTH AND HUMAN SERVICES.

Not later than 7 days after the date of the enactment of this Act, the Secretary of Health and Human Services shall respond in full to the following congressional inquiries:

(1) The letter dated February 28, 2012, from the Chairman and Ranking Member of the Subcommittee on Contracting Oversight of

the Committee on Homeland Security and Governmental Affairs of the Senate, requesting certain information regarding Department of Health and Human Services contracts for the acquisition of public relations, publicity, advertising, communications, or similar services.

(2) The follow-up letter dated May 22, 2012, from the Ranking Member of the Subcommittee on Contracting Oversight of the Committee on Homeland Security and Governmental Affairs of the Senate, requesting information regarding a reported $20,000,000 Department of Health and Human Services contract with a public relations firm.

SA 2699. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

TITLE ____—REPEAL OF PPACA

SEC. __01. SHORT TITLE.

This title may be cited as the ''Repealing the Job-Killing Health Care Law Act''.

SEC. __02. REPEAL OF THE JOB-KILLING HEALTH CARE LAW AND HEALTH CARE-RELATED PROVISIONS IN THE HEALTH CARE AND EDUCATION RECONCILIATION ACT OF 2010.

(a) JOB-KILLING HEALTH CARE LAW.—Effective as of the enactment of Public Law 111–148, such Act is repealed, and the provisions of law amended or repealed by such Act are restored or revived as if such Act had not been enacted.

(b) HEALTH CARE-RELATED PROVISIONS IN THE HEALTH CARE AND EDUCATION RECONCILIATION ACT OF 2010.—Effective as of the enactment of the Health Care and Education Reconciliation Act of 2010 (Public Law 111–152), title I and subtitle B of title II of such Act are repealed, and the provisions of law amended or repealed by such title or subtitle, respectively, are restored or revived as if such title and subtitle had not been enacted.

SEC. __03. BUDGETARY EFFECTS OF THIS ACT.

The budgetary effects of this title, for the purpose of complying with the Statutory Pay-As-You-Go Act of 2010, shall be determined by reference to the latest statement titled ''Budgetary Effects of PAYGO Legislation'' for this title, submitted for printing in the Congressional Record by the Chairman of the Committee on the Budget of the House of Representatives, as long as such statement has been submitted prior to the vote on passage of this Act.

SA 2700. Mr. ROCKEFELLER (for himself, Mrs. FEINSTEIN, and Mr. PRYOR) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 212, after line 6, add the following:

TITLE VIII—DATA SECURITY AND BREACH NOTIFICATION

SEC. 801. SHORT TITLE.

This title may be cited as the ''Data Security and Breach Notification Act of 2012''.

SEC. 802. REQUIREMENTS FOR INFORMATION SECURITY.

(a) GENERAL SECURITY POLICIES AND PROCEDURES.—

(1) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to require each covered entity that owns or possesses data containing personal information, or contracts to have any third-party entity maintain such data for such covered entity, to establish and implement policies and procedures regarding information security practices for the treatment and protection of personal information taking into consideration—

(A) the size of, and the nature, scope, and complexity of the activities engaged in by such covered entity;

(B) the current state of the art in administrative, technical, and physical safeguards for protecting such information;

(C) the cost of implementing the safeguards under subparagraph (B); and

(D) the impact on small businesses and nonprofits.

(2) REQUIREMENTS.—The regulations shall require the policies and procedures to include the following:

(A) A security policy with respect to the collection, use, sale, other dissemination, and maintenance of personal information.

(B) The identification of an officer or other individual as the point of contact with responsibility for the management of information security.

(C) A process for identifying and assessing any reasonably foreseeable vulnerabilities in each system maintained by the covered entity that contains such personal information, which shall include regular monitoring for a breach of security of each such system.

(D) A process for taking preventive and corrective action to mitigate any vulnerabilities identified in the process required by subparagraph (C), which may include implementing any changes to security practices and the architecture, installation, or implementation of network or operating software.

(E) A process for disposing of data in electronic form containing personal information by shredding, permanently erasing, or otherwise modifying the personal information contained in such data to make such personal information permanently unreadable or indecipherable.

(F) A standard method or methods for the destruction of paper documents and other non-electronic data containing personal information.

(b) LIMITATIONS.—

(1) COVERED ENTITIES SUBJECT TO THE GRAMM-LEACH-BLILEY ACT.—Notwithstanding section 805 of this Act, this section (and any regulations issued pursuant to this section) shall not apply to any financial institution that is subject to title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) with respect to covered information under that Act.

(2) APPLICABILITY OF OTHER INFORMATION SECURITY REQUIREMENTS.—To the extent that the information security requirements of section 13401 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931) or of section 1173(d) of title XI, part C of the Social Security Act (42 U.S.C. 1320d-2(d)) apply in any circumstance to a person who is subject to either of those Acts, and to the extent the person is acting as an entity subject to either of those Acts, the person shall be exempt from the requirements of this section with respect to any data governed by section 13401 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931) or by the Health Insurance Portability and Accountability Act of 1996 Security Rule (45 C.F.R. 160.103 and Part 164).

(3) CERTAIN SERVICE PROVIDERS.—Nothing in this section shall apply to a service provider for any electronic communication by a third party to the extent that the service provider is engaged in the transmission, routing, or temporary, intermediate, or transient storage of that communication.

SEC. 803. NOTIFICATION OF BREACH OF SECURITY.

(a) NATIONWIDE NOTIFICATION.—A covered entity that owns or possesses data in electronic form containing personal information, following the discovery of a breach of security of the system maintained by the covered entity that contains such data, shall notify—

(1) each individual who is a citizen or resident of the United States and whose personal information was or is reasonably believed to have been acquired or accessed from the covered entity as a result of the breach of security; and

(2) the Commission, unless the covered entity has notified the designated entity under section 804.

(b) SPECIAL NOTIFICATION REQUIREMENTS.—

(1) THIRD-PARTY ENTITIES.—In the event of a breach of security of a system maintained by a third-party entity that has been contracted to maintain or process data in electronic form containing personal information on behalf of any other covered entity who owns or possesses such data, the third-party entity shall notify the covered entity of the breach of security. Upon receiving notification from the third party entity, such covered entity shall provide the notification required under subsection (a).

(2) SERVICE PROVIDERS.—If a service provider becomes aware of a breach of security of data in electronic form containing personal information that is owned or possessed by another covered entity that connects to or uses a system or network provided by the service provider for the purpose of transmitting, routing, or providing intermediate or transient storage of such data, the service provider shall notify of the breach of security only the covered entity who initiated such connection, transmission, routing, or storage if such covered entity can be reasonably identified. Upon receiving the notification from the service provider, the covered entity shall provide the notification required under subsection (a).

(3) COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.—If a covered entity is required to provide notification to more than 5,000 individuals under subsection (a)(1), the covered entity also shall notify each major credit reporting agency of the timing and distribution of the notices, except when the only personal information that is the subject of the breach of security is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code. Such notice shall be given to each credit reporting agency without unreasonable delay and, if it will not delay notice to the affected individuals, prior to the distribution of notices to the affected individuals.

(c) TIMELINESS OF NOTIFICATION.—Notification under subsection (a) shall be made—

(1) not later than 45 days after the date of discovery of a breach of security; or

(2) as promptly as possible if the covered entity providing notice can show that providing notice within the time frame under paragraph (1) is not feasible due to circumstances necessary—

(A) to accurately identify affected consumers;

(B) to prevent further breach or unauthorized disclosures; or

(C) to reasonably restore the integrity of the data system.

(d) METHOD AND CONTENT OF NOTIFICATION.—

(1) DIRECT NOTIFICATION.—

(A) METHOD OF DIRECT NOTIFICATION.—A covered entity shall be in compliance with the notification requirement under subsection (a)(1) if—

(i) the covered entity provides conspicuous and clearly identified notification—

(I) in writing; or

(II) by e-mail or other electronic means if—

(aa) the covered entity's primary method of communication with the individual is by e-mail or such other electronic means; or

(bb) the individual has consented to receive notification by e-mail or such other electronic means and such notification is provided in a manner that is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001); and

(ii) the method of notification selected under clause (i) can reasonably be expected to reach the intended individual.

(B) CONTENT OF DIRECT NOTIFICATION.—Each method of direct notification under subparagraph (A) shall include—

(i) the date, estimated date, or estimated date range of the breach of security;

(ii) a description of the personal information that was or is reasonably believed to have been acquired or accessed as a result of the breach of security;

(iii) a telephone number that an individual can use at no cost to the individual to contact the covered entity to inquire about the breach of security or the information the covered entity maintained about that individual;

(iv) notice that the individual may be entitled to consumer credit reports under subsection (e)(1);

(v) instructions how an individual can request consumer credit reports under subsection (e)(1);

(vi) a telephone number, that an individual can use at no cost to the individual, and an address to contact each major credit reporting agency; and

(vii) a telephone number, that an individual can use at no cost to the individual, and an Internet Web site address to obtain information regarding identity theft from the Commission.

(2) SUBSTITUTE NOTIFICATION.—

(A) CIRCUMSTANCES GIVING RISE TO SUBSTITUTE NOTIFICATION.—A covered entity required to provide notification to individuals under subsection (a)(1) may provide substitute notification instead of direct notification under paragraph (1)—

(i) if direct notification is not feasible due to lack of sufficient contact information for the individual required to be notified; or

(ii) if the covered entity owns or possesses data in electronic form containing personal information of fewer than 10,000 individuals and direct notification is not feasible due to excessive cost to the covered entity required to provide such notification relative to the resources of such covered entity, as determined in accordance with the regulations issued by the Commission under paragraph (3)(A).

(B) METHOD OF SUBSTITUTE NOTIFICATION.—Substitute notification under this paragraph shall include—

(i) conspicuous and clearly identified notification by e-mail to the extent the covered entity has an e-mail address for an individual who is entitled to notification under subsection (a)(1);

(ii) conspicuous and clearly identified notification on the Internet Web site of the covered entity if the covered entity maintains an Internet Web site; and

(iii) notification to print and to broadcast media, including major media in metropolitan and rural areas where the individuals whose personal information was acquired reside.

(C) CONTENT OF SUBSTITUTE NOTIFICATION.—Each method of substitute notification under this paragraph shall include—

(i) the date, estimated date, or estimated date range of the breach of security;

(ii) a description of the types of personal information that were or are reasonably believed to have been acquired or accessed as a result of the breach of security;

(iii) notice that an individual may be entitled to consumer credit reports under subsection (e)(1);

(iv) instructions how an individual can request consumer credit reports under subsection (e)(1);

(v) a telephone number that an individual can use at no cost to the individual to learn whether the individual's personal information is included in the breach of security;

(vi) a telephone number, that an individual can use at no cost to the individual, and an address to contact each major credit reporting agency; and

(vii) a telephone number, that an individual can use at no cost to the individual, and an Internet Web site address to obtain information regarding identity theft from the Commission.

(3) REGULATIONS AND GUIDANCE.—

(A) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall, by regulation under section 553 of title 5, United States Code, establish criteria for determining circumstances under which substitute notification may be provided under section 803(d)(2) of this Act, including criteria for determining if direct notification under section 803(d)(1) of this Act is not feasible due to excessive costs to the covered entity required to provided such notification relative to the resources of such covered entity. The regulations may also identify other circumstances where substitute notification would be appropriate for any covered entity, including circumstances under which the cost of providing direct notification exceeds the benefits to consumers.

(B) GUIDANCE.—In addition, the Commission, in consultation with the Small Business Administration, shall provide and publish general guidance with respect to compliance with this subsection. The guidance shall include—

(i) a description of written or e-mail notification that complies with paragraph (1); and

(ii) guidance on the content of substitute notification under paragraph (2), including the extent of notification to print and broadcast media that complies with paragraph (2)(B)(iii).

(e) OTHER OBLIGATIONS FOLLOWING BREACH.—

(1) IN GENERAL.—Not later than 60 days after the date of request by an individual whose personal information was included in a breach of security and quarterly thereafter for 2 years, a covered entity required to provide notification under subsection (a)(1) shall provide, or arrange for the provision of, to the individual at no cost, consumer credit reports from at least 1 major credit reporting agency.

(2) LIMITATION.—Paragraph (1) shall not apply if the only personal information that is the subject of the breach of security is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code.

(3) RULEMAKING.—The Commission's rulemaking under subsection (d)(3) shall include—

(A) determination of the circumstances under which a covered entity required to provide notification under subsection (a) must provide or arrange for the provision of free consumer credit reports; and

(B) establishment of a simple process under which a covered entity that is a small business or small non-profit organization may request a full or a partial waiver or a modified or an alternative means of complying with this subsection if providing free consumer credit reports is not feasible due to excessive costs relative to the resources of such covered entity and relative to the level of harm, to affected individuals, caused by the breach of security.

(f) DELAY OF NOTIFICATION AUTHORIZED FOR NATIONAL SECURITY AND LAW ENFORCEMENT PURPOSES.—

(1) IN GENERAL.—If the United States Secret Service or the Federal Bureau of Investigation determines that notification under this section would impede a criminal investigation or a national security activity, notification shall be delayed upon written notice from the United States Secret Service or the Federal Bureau of Investigation to the covered entity that experienced the breach of security. Written notice from the United States Secret Service or the Federal Bureau of Investigation shall specify the period of delay requested for national security or law enforcement purposes.

(2) SUBSEQUENT DELAY OF NOTIFICATION.—

(A) IN GENERAL.—A covered entity shall provide notification under this section not later than 30 days after the day that the delay was invoked unless a Federal law enforcement or intelligence agency provides subsequent written notice to the covered entity that further delay is necessary.

(B) WRITTEN JUSTIFICATION REQUIREMENTS.—

(i) UNITED STATES SECRET SERVICE.—If the United States Secret Service instructs a covered entity to delay notification under this section beyond the 30 day period under subparagraph (A) (''subsequent delay''), the United States Secret Service shall submit written justification for the subsequent delay to the Secretary of Homeland Security before the subsequent delay begins.

(ii) FEDERAL BUREAU OF INVESTIGATION.—If the Federal Bureau of Investigation instructs a covered entity to delay notification under this section beyond the 30 day period under subparagraph (A) (''subsequent delay''), the Federal Bureau of Investigation shall submit written justification for the subsequent delay to the U.S. Attorney General before the subsequent delay begins.

(3) LAW ENFORCEMENT IMMUNITY.—No cause of action shall lie in any court against any Federal agency for acts relating to the delay of notification for national security or law enforcement purposes under this title.

(g) GENERAL EXEMPTION.—

(1) IN GENERAL.—A covered entity shall be exempt from the requirements under this section if, following a breach of security, the covered entity determines that there is no reasonable risk of identity theft, fraud, or other unlawful conduct.

(2) PRESUMPTION.—

(A) IN GENERAL.—There shall be a presumption that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security if—

(i) the data is rendered unusable, unreadable, or indecipherable through a security technology or methodology; and

(ii) the security technology or methodology under clause (i) is generally accepted by experts in the information security field.

(B) REBUTTAL.—The presumption under subparagraph (A) may be rebutted by facts demonstrating that the security technology or methodology in a specific case has been or is reasonably likely to be compromised.

(3) TECHNOLOGIES OR METHODOLOGIES.—Not later than 1 year after the date of enactment

of this Act, and biannually thereafter, the Commission, after consultation with the National Institute of Standards and Technology, shall issue rules (pursuant to section 553 of title 5, United States Code) or guidance to identify each security technology and methodology under paragraph (2). In issuing the rules or guidance, the Commission shall—

(A) consult with relevant industries, consumer organizations, data security and identity theft prevention experts, and established standards setting bodies; and

(B) consider whether and in what circumstances a security technology or methodology currently in use, such as encryption, complies with the standards under paragraph (2).

(4) FTC GUIDANCE.—Not later than 1 year after the date of enactment of this Act, the Commission, after consultation with the National Institute of Standards and Technology, shall issue guidance regarding the application of the exemption under paragraph (1).

(h) EXEMPTIONS FOR NATIONAL SECURITY AND LAW ENFORCEMENT PURPOSES.—

(1) IN GENERAL.—A covered entity shall be exempt from the requirements under this section if—

(A) a determination is made—

(i) by the United States Secret Service or the Federal Bureau of Investigation that notification of the breach of security could be reasonably expected to reveal sensitive sources and methods or similarly impede the ability of the Government to conduct law enforcement or intelligence investigations; or

(ii) by the Federal Bureau of Investigation that notification of the breach of security could be reasonably expected to cause damage to the national security; and

(B) the United States Secret Service or the Federal Bureau of Investigation, as the case may be, provides written notice of its determination under subparagraph (A) to the covered entity.

(2) UNITED STATES SECRET SERVICE.—If the United States Secret Service invokes an exemption under paragraph (1), the United States Secret Service shall submit written justification for invoking the exemption to the Secretary of Homeland Security before the exemption is invoked.

(3) FEDERAL BUREAU OF INVESTIGATION.—If the Federal Bureau of Investigation invokes an exemption under paragraph (1), the Federal Bureau of Investigation shall submit written justification for invoking the exemption to the U.S. Attorney General before the exemption is invoked.

(4) IMMUNITY.—No cause of action shall lie in any court against any Federal agency for acts relating to the exemption from notification for national security or law enforcement purposes under this title.

(5) REPORTS.—Not later than 18 months after the date of enactment of this Act, and upon request by Congress thereafter, the United States Secret Service and Federal Bureau of Investigation shall submit to Congress a report on the number and nature of breaches of security subject to the exemptions for national security and law enforcement purposes under this subsection.

(i) FINANCIAL FRAUD PREVENTION EXEMPTION.—

(1) IN GENERAL.—A covered entity shall be exempt from the requirements under this section if the covered entity utilizes or participates in a security program that—

(A) effectively blocks the use of the personal information to initiate an unauthorized financial transaction before it is charged to the account of the individual; and

(B) provides notice to each affected individual after a breach of security that resulted in attempted fraud or an attempted unauthorized transaction.

(2) LIMITATIONS.—An exemption under paragraph (1) shall not apply if—

(A) the breach of security includes personal information, other than a credit card number or credit card security code, of any type; or

(B) the breach of security includes both the individual's credit card number and the individual's first and last name.

(j) FINANCIAL INSTITUTIONS REGULATED BY FEDERAL FUNCTIONAL REGULATORS.—

(1) IN GENERAL.—Nothing in this section shall apply to a covered financial institution if the Federal functional regulator with jurisdiction over the covered financial institution has issued a standard by regulation or guideline under title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) that—

(A) requires financial institutions within its jurisdiction to provide notification to individuals following a breach of security; and

(B) provides protections substantially similar to, or greater than, those required under this title.

(2) DEFINITIONS.—In this subsection—

(A) the term ''covered financial institution'' means a financial institution that is subject to—

(i) the data security requirements of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.);

(ii) any implementing standard issued by regulation or guideline issued under that Act; and

(iii) the jurisdiction of a Federal functional regulator under that Act;

(B) the term ''Federal functional regulator'' has the meaning given the term in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809); and

(C) the term ''financial institution'' has the meaning given the term in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809).

(k) EXEMPTION; HEALTH PRIVACY.—

(1) COVERED ENTITY OR BUSINESS ASSOCIATE UNDER HITECH ACT.—To the extent that a covered entity under this title acts as a covered entity or a business associate under section 13402 of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17932), and has the obligation to provide breach notification under that Act or its implementing regulations, the requirements of this section shall not apply.

(2) ENTITY SUBJECT TO HITECH ACT.—To the extent that a covered entity under this title acts as a vendor of personal health records, a third party service provider, or other entity subject to section 13407 of the Health Information Technology for Economical and Clinical Health Act (42 U.S.C. 17937), and has the obligation to provide breach notification under that Act or its implementing regulations, the requirements of this section shall not apply.

(3) LIMITATION OF STATUTORY CONSTRUCTION.—Nothing in this Act may be construed in any way to give effect to the sunset provision under section 13407(g)(2) of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17937(g)(2)) or to otherwise limit or affect the applicability, under section 13407 of that Act, of the breach notification requirement for vendors of personal health records and each entity described in clause (ii), (iii), or (iv) of section 13424(b)(1)(A) of that Act (42 U.S.C. 17953(b)(1)(A)) .

(l) WEB SITE NOTICE OF FEDERAL TRADE COMMISSION.—If the Commission, upon receiving notification of any breach of security that is reported to the Commission, finds that notification of the breach of security via the Commission's Internet Web site would be in the public interest or for the protection of consumers, the Commission shall place such a notice in a clear and conspicuous location on its Internet Web site.

(m) FTC STUDY ON NOTIFICATION IN LANGUAGES IN ADDITION TO ENGLISH.—Not later than 1 year after the date of enactment of this Act, the Commission shall conduct a study on the practicality and cost effectiveness of requiring the direct notification required by subsection (d)(1) to be provided in a language in addition to English to individuals known to speak only such other language.

(n) GENERAL RULEMAKING AUTHORITY.—The Commission may promulgate regulations necessary under section 553 of title 5, United States Code, to effectively enforce the requirements of this section.

SEC. 804. NOTICE TO LAW ENFORCEMENT.

(a) DESIGNATION OF GOVERNMENT ENTITY TO RECEIVE NOTICE.—Not later than 60 days after the date of enactment of this Act, the Secretary of the Department of Homeland Security shall designate a Federal Government entity to receive notice under this section.

(b) NOTICE.—A covered entity shall notify the designated entity of a breach of security if—

(1) the number of individuals whose personal information was, or is reasonably believed to have been, acquired or assessed as a result of the breach of security exceeds 10,000;

(2) the breach of security involves a database, networked or integrated databases, or other data system containing the personal information of more than 1,000,000 individuals;

(3) the breach of security involves databases owned by the Federal Government; or

(4) the breach of security involves primarily personal information of individuals known to the covered entity to be employees or contractors of the Federal Government involved in national security or law enforcement.

(c) CONTENT OF NOTICES.—

(1) IN GENERAL.—Each notice under subsection (b) shall contain—

(A) the date, estimated date, or estimated date range of the breach of security;

(B) a description of the nature of the breach of security;

(C) a description of each type of personal information that was or is reasonably believed to have been acquired or accessed as a result of the breach of security; and

(D) a statement of each paragraph under subsection (b) that applies to the breach of security.

(2) CONSTRUCTION.—Nothing in this section shall be construed to require a covered entity to reveal specific or identifying information about an individual as part of the notice under paragraph (1).

(d) RESPONSIBILITIES OF THE DESIGNATED ENTITY.—The designated entity shall promptly provide each notice it receives under subsection (b) to—

(1) the United States Secret Service;

(2) the Federal Bureau of Investigation;

(3) the Federal Trade Commission;

(4) the United States Postal Inspection Service, if the breach of security involves mail fraud;

(5) the attorney general of each State affected by the breach of security; and

(6) as appropriate, other Federal agencies for law enforcement, national security, or data security purposes.

(e) TIMING OF NOTICES.—Notice under this section shall be delivered as follows:

(1) Notice under subsection (b) shall be delivered as promptly as possible, but—

(A) not less than 3 business days before notification to an individual pursuant to section 803; and

(B) not later than 10 days after the date of discovery of the events requiring notice.

(2) Notice under subsection (d) shall be delivered as promptly as possible, but not later than 1 business day after the date that the designated entity receives notice of a breach of security from a covered entity.

SEC. 805. APPLICATION AND ENFORCEMENT.

(a) GENERAL APPLICATION.—The requirements of sections 802 and 803 apply to—

(1) those persons, partnerships, or corporations over which the Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)); and

(2) notwithstanding sections 4 and 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 44 and 45(a)(2)), any non-profit organization, including any organization described in section 501(c) of the Internal Revenue Code of 1986 that is exempt from taxation under section 501(a) of the Internal Revenue Code of 1986.

(b) OPT-IN FOR CERTAIN OTHER ENTITIES.—

(1) IN GENERAL.—Section 803 shall apply to any other person or entity that enters into an agreement with the Commission under which section 803 would apply to that person or entity, with respect to any acts or omissions that occur while the agreement is in effect and that may constitute a violation of section 803, if—

(A) not less than 30 days prior to entering into the agreement with the person or entity, the Commission publishes notice in the Federal Register of the Commission's intent to enter into the agreement; and

(B) not later than 14 business days after entering into the agreement with the person or entity, the Commission publishes in the Federal Register—

(i) notice of the agreement;

(ii) the identify of each person or entity covered by the agreement; and

(iii) the effective date of the agreement.

(2) CONSTRUCTION.—

(A) OTHER FEDERAL LAW.—An agreement under paragraph (1) shall not effect a person's obligation or an entity's obligation to provide notice of a breach of security or similar event under any other Federal law.

(B) NO PREEMPTION PRIOR TO VALID AGREEMENT.—Subsections (a)(2) and (b) of section 807 shall not apply to a breach of security that occurs before a valid agreement under paragraph (1) is in effect.

(c) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 802 or 803 of this Act shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(2) POWERS OF COMMISSION.—The Commission shall enforce this title in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this title. Any covered entity who violates such regulations shall be subject to the penalties and entitled to the privileges and immunities provided in that Act.

(3) LIMITATION.—In promulgating rules under this title, the Commission shall not require the deployment or use of any specific products or technologies, including any specific computer software or hardware.

(d) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) CIVIL ACTION.—In any case in which the attorney general of a State, or an official or agency of a State, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any covered entity who violates section 802 or 803 of this Act, the attorney general, official, or agency of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction—

(A) to enjoin further violation of such section by the defendant;

(B) to compel compliance with such section; or

(C) to obtain civil penalties in the amount determined under paragraph (2).

(2) CIVIL PENALTIES.—

(A) CALCULATION.—

(i) TREATMENT OF VIOLATIONS OF SECTION 802.—For purposes of paragraph (1)(C) with regard to a violation of section 802, the amount determined under this paragraph is the amount calculated by multiplying the number of days that a covered entity is not in compliance with such section by an amount not greater than $11,000.

(ii) TREATMENT OF VIOLATIONS OF SECTION 803.—For purposes of paragraph (1)(C) with regard to a violation of section 803, the amount determined under this paragraph is the amount calculated by multiplying the number of violations of such section by an amount not greater than $11,000. Each failure to send notification as required under section 803 to a resident of the State shall be treated as a separate violation.

(B) ADJUSTMENT FOR INFLATION.—Beginning on the date that the Consumer Price Index is first published by the Bureau of Labor Statistics that is after 1 year after the date of enactment of this Act, and each year thereafter, the amounts specified in clauses (i) and (ii) of subparagraph (A) and in clauses (i) and (ii) of subparagraph (C) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

(C) MAXIMUM TOTAL LIABILITY.—Notwithstanding the number of actions which may be brought against a covered entity under this subsection, the maximum civil penalty for which any covered entity may be liable under this subsection shall not exceed—

(i) $5,000,000 for each violation of section 802; and

(ii) $5,000,000 for all violations of section 803 resulting from a single breach of security.

(3) INTERVENTION BY THE FTC.—

(A) NOTICE AND INTERVENTION.—The State shall provide prior written notice of any action under paragraph (1) to the Commission and provide the Commission with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case the State shall serve such notice immediately upon commencing such action. The Commission shall have the right—

(i) to intervene in the action;

(ii) upon so intervening, to be heard on all matters arising therein; and

(iii) to file petitions for appeal.

(B) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING.—If the Commission has instituted a civil action for violation of this title, no State attorney general, or official or agency of a State, may bring an action under this subsection during the pendency of that action against any defendant named in the complaint of the Commission for any violation of this title alleged in the complaint.

(4) CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this title shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State—

(A) to conduct investigations;

(B) to administer oaths or affirmations; or

(C) to compel the attendance of witnesses or the production of documentary and other evidence.

(e) AFFIRMATIVE DEFENSE FOR A VIOLATION OF SECTION 803.—It shall be an affirmative defense to an enforcement action brought under subsection (c), or a civil action brought under subsection (d), based on a violation of section 803, that all of the personal information contained in the data in electronic form that was acquired or accessed as a result of a breach of security of the defendant is public record information that is lawfully made available to the general public from Federal, State, or local government records and was acquired by the defendant from such records.

(f) NOTICE TO LAW ENFORCEMENT; CIVIL ENFORCEMENT BY ATTORNEY GENERAL.—

(1) IN GENERAL.—The Attorney General may bring a civil action in the appropriate United States district court against any covered entity that engages in conduct constituting a violation of section 804.

(2) PENALTIES.—

(A) IN GENERAL.—Upon proof of such conduct by a preponderance of the evidence, a covered entity shall be subject to a civil penalty of not more than $1,000 per individual whose personal information was or is reasonably believed to have been accessed or acquired as a result of the breach of security that is the basis of the violation, up to a maximum of $100,000 per day while such violation persists.

(B) LIMITATIONS.—The total amount of the civil penalty assessed under this subsection against a covered entity for acts or omissions relating to a single breach of security shall not exceed $1,000,000, unless the conduct constituting a violation of section 804 was willful or intentional, in which case an additional civil penalty of up to $1,000,000 may be imposed.

(C) ADJUSTMENT FOR INFLATION.—Beginning on the date that the Consumer Price Index is first published by the Bureau of Labor Statistics that is after 1 year after the date of enactment of this Act, and each year thereafter, the amounts specified in subparagraphs (A) and (B) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

(3) INJUNCTIVE ACTIONS.—If it appears that a covered entity has engaged, or is engaged, in any act or practice that constitutes a violation of section 804, the Attorney General may petition an appropriate United States district court for an order enjoining such practice or enforcing compliance with section 804.

(4) ISSUANCE OF ORDER.—A court may issue such an order under paragraph (3) if it finds that the conduct in question constitutes a violation of section 804.

(g) CONCEALMENT OF BREACHES OF SECURITY.—

(1) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by adding at the end the following:

"§ 1041. Concealment of breaches of security involving personal information

''(a) IN GENERAL.—Any person who, having knowledge of a breach of security and of the fact that notification of the breach of security is required under the Data Security and Breach Notification Act of 2012, intentionally and willfully conceals the fact of the breach of security, shall, in the event that the breach of security results in economic harm to any individual in the amount of $1,000 or more, be fined under this title, imprisoned for not more than 5 years, or both.

''(b) PERSON DEFINED.—For purposes of subsection (a), the term 'person' has the same meaning as in section 1030(e)(12) of this title.

''(c) ENFORCEMENT AUTHORITY.—

''(1) IN GENERAL.—The United States Secret Service and the Federal Bureau of Investigation shall have the authority to investigate offenses under this section.

''(2) CONSTRUCTION.—The authority granted in paragraph (1) shall not be exclusive of any existing authority held by any other Federal agency.''.

(2) CONFORMING AND TECHNICAL AMENDMENTS.—The table of sections for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

''1041. Concealment of breaches of security involving personal information.''.

SEC. 806. DEFINITIONS.

In this title:

(1) BREACH OF SECURITY.—

(A) IN GENERAL.—The term ''breach of security'' means compromise of the security, confidentiality, or integrity of, or loss of, data in electronic form that results in, or there is a reasonable basis to conclude has resulted in, unauthorized access to or acquisition of personal information from a covered entity.

(B) EXCLUSIONS.—The term'' breach of security'' does not include—

(i) a good faith acquisition of personal information by a covered entity, or an employee or agent of a covered entity, if the personal information is not subject to further use or unauthorized disclosure;

(ii) any lawfully authorized investigative, protective, or intelligence activity of a law enforcement or an intelligence agency of the United States, a State, or a political subdivision of a State; or

(iii) the release of a public record not otherwise subject to confidentiality or nondisclosure requirements.

(2) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(3) COVERED ENTITY.—The term ''covered entity'' means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity, and any charitable, educational, or nonprofit organization, that acquires, maintains, or utilizes personal information.

(4) DATA IN ELECTRONIC FORM.—The term ''data in electronic form'' means any data stored electronically or digitally on any computer system or other database, including recordable tapes and other mass storage devices.

(5) DESIGNATED ENTITY.—The term ''designated entity'' means the Federal Government entity designated by the Secretary of Homeland Security under section 804.

(6) ENCRYPTION.—The term ''encryption'' means the protection of data in electronic form in storage or in transit using an encryption technology that has been adopted by an established standards setting body which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data. Such encryption must include appropriate management and safeguards of such keys to protect the integrity of the encryption.

(7) IDENTITY THEFT.—The term ''identity theft'' means the unauthorized use of another person's personal information for the purpose of engaging in commercial transactions under the identity of such other person, including any contact that violates section 1028A of title 18, United States Code.

(8) MAJOR CREDIT REPORTING AGENCY.—The term ''major credit reporting agency'' means a consumer reporting agency that compiles and maintains files on consumers on a nationwide basis within the meaning of section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

(9) PERSONAL INFORMATION.—

(A) DEFINITION.—The term ''personal information'' means any information or compilation of information in electronic or digital form that includes—

(i) a financial account number or credit or debit card number in combination with any security code, access code, or password that is required for an individual to obtain credit, withdraw funds, or engage in a financial transaction; or

(ii) an individual's first and last name or first initial and last name in combination with—

(I) a non-truncated social security number, driver's license number, passport number, or alien registration number, or other similar number issued on a government document used to verify identity;

(II) unique biometric data such as a finger print, voice print, retina or iris image, or any other unique physical representation;

(III) a unique account identifier, electronic identification number, user name, or routing code in combination with any associated security code, access code, or password that is required for an individual to obtain money, goods, services, or any other thing of value; or

(IV) 2 of the following:

(aa) Home address or telephone number.

(bb) Mother's maiden name, if identified as such.

(cc) Month, day, and year of birth.

(B) MODIFIED DEFINITION BY RULEMAKING.—If the Commission determines that the definition under subparagraph (A) is not reasonably sufficient to protect individuals from identify theft, fraud, or other unlawful conduct, the Commission by rule promulgated under section 553 of title 5, United States Code, may modify the definition of ''personal information'' under subparagraph (A) to the extent the modification will not unreasonably impede interstate commerce.

(10) PUBLIC RECORD INFORMATION.—The term ''public record information'' means information about an individual which has been obtained originally from records of a Federal, State, or local government entity that are available for public inspection.

(11) SERVICE PROVIDER.—The term ''service provider'' means a person that provides electronic data transmission, routing, intermediate and transient storage, or connections to its system or network, where the person providing such services does not select or modify the content of the electronic data, is not the sender or the intended recipient of the data, and does not differentiate personal information from other information that such person transmits, routes, or stores, or for which such person provides connections. Any such person shall be treated as a service provider under this title only to the extent that it is engaged in the provision of such transmission, routing, intermediate and transient storage, or connections.

SEC. 807. EFFECT ON OTHER LAWS.

(a) PREEMPTION OF STATE INFORMATION SECURITY LAWS.—This title supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State, with respect to those entities covered by the regulations issued pursuant to this title, that expressly—

(1) requires information security practices and treatment of data containing personal information similar to any of those required under section 802; or

(2) requires notification to individuals of a breach of security as defined in section 806.

(b) ADDITIONAL PREEMPTION.—

(1) IN GENERAL.—No person other than a person specified in section 805(d) may bring a civil action under the laws of any State if such action is premised in whole or in part upon the defendant violating any provision of this title.

(2) PROTECTION OF CONSUMER PROTECTION LAWS.—Except as provided in subsection (a) of this section, this subsection shall not be construed to limit the enforcement of any State consumer protection law by an attorney general of a State.

(c) PROTECTION OF CERTAIN STATE LAWS.—This title shall not be construed to preempt the applicability of—

(1) State trespass, contract, or tort law; or

(2) any other State laws to the extent that those laws relate to acts of fraud.

(d) PRESERVATION OF FTC AUTHORITY.—Nothing in this title may be construed in any way to limit or affect the Commission's authority under any other provision of law.

SEC. 808. APPLICABILITY OF SECTION 631 OF THE COMMUNICATIONS ACT OF 1934.

(a) IN GENERAL.—To the extent that a cable operator (as defined under section 631 of the Communications Act of 1934 (47 U.S.C. 551)) is subject to a requirement regarding personal information (as defined in section 806 of this Act)—

(1) under this title that is in conflict with a requirement under section 631 of the Communications Act of 1934 (47 U.S.C. 551), each applicable section of this Act shall control (including enforcement); and

(2) under section 631 of the Communications Act of 1934 (47 U.S.C. 551) that is in addition to or different from a requirement under this title, each applicable subsection of section 631 of the Communications Act of 1934 (47 U.S.C. 551) shall remain in effect (including enforcement and right of action).

(b) LIMITATION OF STATUTORY CONSTRUCTION.—Nothing in this title shall preclude the application of section 631 of the Communications Act of 1934 (47 U.S.C. 551), to information that is not included in the definition of personal information under section 806 of this Act.

SEC. 809. EFFECTIVE DATE.

This title shall take effect 1 year after the date of enactment of this Act.

SA 2701. Mr. FRANKEN (for himself, Mr. PAUL, Mr. WYDEN, Mr. AKAKA, Mr. COONS, Mr. BLUMENTHAL, Mr. SANDERS, Mr. UDALL of New Mexico, Mr. MERKLEY, Mr. SCHUMER, Ms. CANTWELL, Mrs. SHAHEEN, Mr. BEGICH, Mr. DURBIN, and Mr. HARKIN) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Strike section 701.

SA 2702. Mr. FRANKEN (for himself, Mr. PAUL, Mr. WYDEN, Mr. AKAKA, Mr. COONS, Mr. BLUMENTHAL, Mr. SANDERS, Mr. UDALL of New Mexico, Mr. MERKLEY, Mr. SCHUMER, Ms. CANTWELL, Mrs. SHAHEEN, Mr. BEGICH, Mr. DURBIN, and Mr. HARKIN) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 169, strike line 15 and all that follows through page 172, line 25.

Page 189, beginning on line 22, strike ''performing, monitoring, operating countermeasures, or''.

Page 196, strike lines 10, 11, and 12.

Beginning on page 205, strike line 15 and all that follows through page 206, line 2.

SA 2703. Mr. FRANKEN (for himself, Mr. PAUL, Mr. WYDEN, Mr. AKAKA, Mr. COONS, Mr. BLUMENTHAL, Mr. SANDERS, Mr. UDALL of New Mexico, Mr. MERKLEY, Mr. SCHUMER, Ms. CANTWELL, Mrs. SHAHEEN, Mr. BEGICH, Mr. DURBIN, and Mr. HARKIN) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Strike title VII and insert the following:

TITLE VII—INFORMATION SHARING

SEC. 701. VOLUNTARY DISCLOSURE OF CYBERSECURITY THREAT INDICATORS AMONG PRIVATE ENTITIES.

(a) AUTHORITY TO DISCLOSE.—Notwithstanding any other provision of law, any private entity may disclose lawfully obtained cybersecurity threat indicators to any other private entity in accordance with this section.

(b) USE AND PROTECTION OF INFORMATION.—A private entity disclosing or receiving cybersecurity threat indicators pursuant to subsection (a)—

(1) may use, retain, or further disclose such cybersecurity threat indicators solely for the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from cybersecurity threats or mitigating such threats;

(2) shall make reasonable efforts to safeguard communications, records, system traffic, or other information that can be used to identify specific persons from unauthorized access or acquisition;

(3) shall comply with any lawful restrictions placed on the disclosure or use of cybersecurity threat indicators, including, if requested, the removal of information that may be used to identify specific persons from such indicators; and

(4) may not use the cybersecurity threat indicators to gain an unfair competitive advantage to the detriment of the entity that authorized such sharing.

(c) TRANSFERS TO UNRELIABLE PRIVATE ENTITIES PROHIBITED.—A private entity may not disclose cybersecurity threat indicators to another private entity that the disclosing entity knows—

(1) has intentionally or willfully violated the requirements of subsection (b); and

(2) is reasonably likely to violate such requirements.

SEC. 702. CYBERSECURITY EXCHANGES.

(a) DESIGNATION OF CYBERSECURITY EXCHANGES.—The Secretary of Homeland Security, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, shall establish—

(1) a process for designating one or more appropriate civilian Federal entities or non-Federal entities to serve as cybersecurity exchanges to receive and distribute cybersecurity threat indicators;

(2) procedures to facilitate and ensure the sharing of classified and unclassified cybersecurity threat indicators in as close to real time as possible with appropriate Federal entities and non-Federal entities in accordance with this title; and

(3) a process for identifying certified entities to receive classified cybersecurity threat indicators in accordance with paragraph (2).

(b) PURPOSE.—The purpose of a cybersecurity exchange is to receive and distribute, in as close to real time as possible, cybersecurity threat indicators, and to thereby avoid unnecessary and duplicative Federal bureaucracy for information sharing as provided in this title.

(c) REQUIREMENT FOR A LEAD FEDERAL CIVILIAN CYBERSECURITY EXCHANGE.—

(1) IN GENERAL.—The Secretary, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, shall designate a civilian Federal entity as the lead cybersecurity exchange to serve as a focal point within the Federal Government for cybersecurity information sharing among Federal entities and with non-Federal entities.

(2) RESPONSIBILITIES.—The lead Federal civilian cybersecurity exchange designated under paragraph (1) shall—

(A) receive and distribute, in as close to real time as possible, cybersecurity threat indicators in accordance with this title;

(B) facilitate information sharing, interaction, and collaboration among and between—

(i) Federal entities;

(ii) State, local, tribal, and territorial governments;

(iii) private entities;

(iv) academia;

(v) international partners, in consultation with the Secretary of State; and

(vi) other cybersecurity exchanges;

(C) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information lawfully obtained from any source, including alerts, advisories, indicators, signatures, and mitigation and response measures, to appropriate Federal and non-Federal entities in as close to real time as possible, to improve the security and protection of information systems;

(D) coordinate with other Federal and non-Federal entities, as appropriate, to integrate information from Federal and non-Federal entities, including Federal cybersecurity centers, non-Federal network or security operation centers, other cybersecurity exchanges, and non-Federal entities that disclose cybersecurity threat indicators under section 703(a), in as close to real time as possible, to provide situational awareness of the United States information security posture and foster information security collaboration among information system owners and operators;

(E) conduct, in consultation with private entities and relevant Federal and other governmental entities, regular assessments of existing and proposed information sharing models to eliminate bureaucratic obstacles to information sharing and identify best practices for such sharing; and

(F) coordinate with other Federal entities, as appropriate, to compile and analyze information about risks and incidents that threaten information systems, including information voluntarily submitted in accordance with section 703(a) or otherwise in accordance with applicable laws.

(3) SCHEDULE FOR DESIGNATION.—The designation of a lead Federal civilian cybersecurity exchange under paragraph (1) shall be made concurrently with the issuance of the interim policies and procedures under section 703(g)(3)(D).

(d) ADDITIONAL CIVILIAN FEDERAL CYBERSECURITY EXCHANGES.—In accordance with the process and procedures established in subsection (a), the Secretary, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, may designate additional civilian Federal entities to receive and distribute cybersecurity threat indicators, if such entities are subject to the requirements for use, retention, and disclosure of information by a cybersecurity exchange under section 703(b) and the special requirements for Federal entities under section 703(g).

(e) REQUIREMENTS FOR NON-FEDERAL CYBERSECURITY EXCHANGES.—

(1) IN GENERAL.—In considering whether to designate a private entity or any other non-Federal entity as a cybersecurity exchange to receive and distribute cybersecurity threat indicators under section 703, and what entity to designate, the Secretary shall consider the following factors:

(A) The net effect that such designation would have on the overall cybersecurity of the United States.

(B) Whether such designation could substantially improve such overall cybersecurity by serving as a hub for receiving and sharing cybersecurity threat indicators in as close to real time as possible, including the capacity of the non-Federal entity for performing those functions.

(C) The capacity of such non-Federal entity to safeguard cybersecurity threat indicators from unauthorized disclosure and use.

(D) The adequacy of the policies and procedures of such non-Federal entity to protect personally identifiable information from unauthorized disclosure and use.

(E) The ability of the non-Federal entity to sustain operations using entirely non-Federal sources of funding.

(2) REGULATIONS.—The Secretary may promulgate regulations as may be necessary to carry out this subsection.

(f) CONSTRUCTION WITH OTHER AUTHORITIES.—Nothing in this section may be construed to alter the authorities of a Federal cybersecurity center, unless such cybersecurity center is acting in its capacity as a designated cybersecurity exchange.

(g) CONGRESSIONAL NOTIFICATION OF DESIGNATION OF CYBERSECURITY EXCHANGES.—

(1) IN GENERAL.—The Secretary, in coordination with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, shall promptly notify Congress, in writing, of any designation of a cybersecurity exchange under this title.

(2) REQUIREMENT.—Written notification under paragraph (1) shall include a description of the criteria and processes used to make the designation.

SEC. 703. VOLUNTARY DISCLOSURE OF CYBERSECURITY THREAT INDICATORS TO A CYBERSECURITY EXCHANGE.

(a) AUTHORITY TO DISCLOSE.—Notwithstanding any other provision of law, a non-Federal entity may disclose lawfully obtained cybersecurity threat indicators to a cybersecurity exchange in accordance with this section.

(b) USE, RETENTION, AND DISCLOSURE OF INFORMATION BY A CYBERSECURITY EXCHANGE.—A cybersecurity exchange may only use, retain, or further disclose information provided pursuant to subsection (a)—

(1) in order to protect information systems from cybersecurity threats and to mitigate cybersecurity threats; or

(2) to law enforcement pursuant to subsection (g)(2).

(c) USE AND PROTECTION OF INFORMATION RECEIVED FROM A CYBERSECURITY EXCHANGE.—A non-Federal entity receiving cybersecurity threat indicators from a cybersecurity exchange—

(1) may use, retain, or further disclose such cybersecurity threat indicators solely for the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from cybersecurity threats or mitigating such threats;

(2) shall make reasonable efforts to safeguard communications, records, system traffic, or other information that can be used to

identify specific persons from unauthorized access or acquisition;

(3) shall comply with any lawful restrictions placed on the disclosure or use of cybersecurity threat indicators by the cybersecurity exchange or a third party, if the cybersecurity exchange received such information from the third party, including, if requested, the removal of information that can be used to identify specific persons from such indicators; and

(4) may not use the cybersecurity threat indicators to gain an unfair competitive advantage to the detriment of the third party that authorized such sharing.

(d) EXEMPTION FROM PUBLIC DISCLOSURE.—Any cybersecurity threat indicator disclosed by a non-Federal entity to a cybersecurity exchange pursuant to subsection (a) shall be—

(1) exempt from disclosure under section 552(b)(3) of title 5, United States Code, or any comparable State law; and

(2) treated as voluntarily shared information under section 552 of title 5, United States Code, or any comparable State law.

(e) EXEMPTION FROM EX PARTE LIMITATIONS.—Any cybersecurity threat indicator disclosed by a non-Federal entity to a cybersecurity exchange pursuant to subsection (a) shall not be subject to the rules of any governmental entity or judicial doctrine regarding ex parte communications with a decision making official.

(f) EXEMPTION FROM WAIVER OF PRIVILEGE.—Any cybersecurity threat indicator disclosed by a non-Federal entity to a cybersecurity exchange pursuant to subsection (a) may not be construed to be a waiver of any applicable privilege or protection provided under Federal, State, tribal, or territorial law, including any trade secret protection.

(g) SPECIAL REQUIREMENTS FOR FEDERAL AND LAW ENFORCEMENT ENTITIES.—

(1) RECEIPT, DISCLOSURE AND USE OF CYBERSECURITY THREAT INDICATORS BY A FEDERAL ENTITY.—

(A) AUTHORITY TO RECEIVE AND USE CYBERSECURITY THREAT INDICATORS.—A Federal entity that is not a cybersecurity exchange may receive, retain, and use cybersecurity threat indicators from a cybersecurity exchange in order—

(i) to protect information systems from cybersecurity threats and to mitigate cybersecurity threats; and

(ii) to disclose such cybersecurity threat indicators to law enforcement in accordance with paragraph (2).

(B) AUTHORITY TO DISCLOSE CYBERSECURITY THREAT INDICATORS.—A Federal entity that is not a cybersecurity exchange shall ensure that if disclosing cybersecurity threat indicators to a non-Federal entity under this section, such non-Federal entity shall use or retain such cybersecurity threat indicators in a manner that is consistent with the requirements in—

(i) subsection (b) on the use and protection of information; and

(ii) paragraph (2).

(2) LAW ENFORCEMENT ACCESS AND USE OF CYBERSECURITY THREAT INDICATORS.—

(A) DISCLOSURE TO LAW ENFORCEMENT.—A Federal entity may disclose cybersecurity threat indicators received under this title to a law enforcement entity if—

(i) the disclosure is permitted under the procedures developed by the Secretary and approved by the Attorney General under paragraph (3); and

(ii) the information appears to pertain—

(I) to a cybersecurity crime which has been, is being, or is about to be committed;

(II) to an imminent threat of death or serious bodily harm; or

(III) to a serious threat to minors, including sexual exploitation and threats to physical safety.

(B) USE BY LAW ENFORCEMENT.—A law enforcement entity may only use cybersecurity threat indicators received by a Federal entity under paragraph (A) in order—

(i) to protect information systems from a cybersecurity threat or investigate, prosecute, or disrupt a cybersecurity crime;

(ii) to protect individuals from an imminent threat of death or serious bodily harm; or

(iii) to protect minors from any serious threat, including sexual exploitation and threats to physical safety.

(3) PRIVACY AND CIVIL LIBERTIES.—

(A) REQUIREMENT FOR POLICIES AND PROCEDURES.—The Secretary, in consultation with privacy and civil liberties experts, the Director of National Intelligence, and the Secretary of Defense, shall develop and periodically review policies and procedures governing the receipt, retention, use, and disclosure of cybersecurity threat indicators by a Federal entity obtained in connection with activities authorized in this title. Such policies and procedures shall—

(i) minimize the impact on privacy and civil liberties, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats;

(ii) reasonably limit the receipt, retention, use and disclosure of cybersecurity threat indicators associated with specific persons consistent with the need to carry out the responsibilities of this title, including establishing a process for the timely destruction of cybersecurity threat indicators that are received pursuant to this section that do not reasonably appear to be related to the purposes identified in paragraph (1)(A);

(iii) include requirements to safeguard cybersecurity threat indicators that may be used to identify specific persons from unauthorized access or acquisition;

(iv) include procedures for notifying entities, as appropriate, if information received pursuant to this section is not a cybersecurity threat indicator; and

(v) protect the confidentiality of cybersecurity threat indicators associated with specific persons to the greatest extent practicable and require recipients to be informed that such indicators may only be used for the purposes identified in paragraph (1)(A).

(B) ADOPTION OF POLICIES AND PROCEDURES.—The head of an agency responsible for a Federal entity designated as a cybersecurity exchange under section 703 shall adopt and comply with the policies and procedures developed under this paragraph.

(C) REVIEW BY THE ATTORNEY GENERAL.—The policies and procedures developed under this subsection shall be provided to the Attorney General for review not later than 1 year after the date of the enactment of this title, and shall not be issued without the Attorney General's approval.

(D) REQUIREMENT FOR INTERIM POLICIES AND PROCEDURES.—The Secretary shall issue interim policies and procedures not later than 60 days after the date of the enactment of this title.

(E) PROVISION TO CONGRESS.—The policies and procedures issued under this title and any amendments to such policies and procedures shall be provided to Congress in an unclassified form and be made public, but may include a classified annex.

(4) OVERSIGHT.—

(A) REQUIREMENT FOR OVERSIGHT.—The Secretary and the Attorney General shall establish a mandatory program to monitor and oversee compliance with the policies and procedures issued under this subsection.

(B) NOTIFICATION OF THE ATTORNEY GENERAL.—The head of each Federal entity that receives information under this title shall—

(i) comply with the policies and procedures developed by the Secretary and approved by the Attorney General under paragraph (3);

(ii) promptly notify the Attorney General of significant violations of such policies and procedures; and

(iii) provide to the Attorney General any information relevant to the violation that the Attorney General requires.

(C) ANNUAL REPORT.—On an annual basis, the Chief Privacy and Civil Liberties Officer of the Department of Justice and the Chief Privacy Officer of the Department, in consultation with the most senior privacy and civil liberties officer or officers of any appropriate agencies, shall jointly submit to Congress a report assessing the privacy and civil liberties impact of the governmental activities conducted pursuant to this title.

(5) REPORTS ON INFORMATION SHARING.—

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

(i) an analysis of the practices of private entities that are disclosing cybersecurity threat indicators pursuant to this title;

(ii) an assessment of the privacy and civil liberties impact of the activities carried out by the Federal entities under this title; and

(iii) recommendations for improvements to or modifications of the law and the policies and procedures established pursuant to paragraph (3) in order to address privacy and civil liberties concerns.

(B) INSPECTORS GENERAL ANNUAL REPORT.—The Inspector General of the Department, the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, and the Inspector General of the Department of Defense shall, on an annual basis, jointly submit to Congress a report on the receipt, use and disclosure of information shared with a Federal cybersecurity exchange under this title, including—

(i) a review of the use by Federal entities of such information for a purpose other than to protect information systems from cybersecurity threats and to mitigate cybersecurity threats, including law enforcement access and use pursuant to paragraph (2);

(ii) a review of the type of information shared with a Federal cybersecurity exchange;

(iii) a review of the actions taken by Federal entities based on such information;

(iv) appropriate metrics to determine the impact of the sharing of such information with a Federal cybersecurity exchange on privacy and civil liberties;

(v) a list of Federal entities receiving such information;

(vi) a review of the sharing of such information among Federal entities to identify inappropriate stovepiping of shared information; and

(vii) any recommendations of the inspectors general for improvements or modifications to the authorities under this title.

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

(6) SANCTIONS.—The head of each Federal entity that conducts activities under this title shall develop and enforce appropriate sanctions for officers, employees, or agents of such entities who conducts such activities—

(A) outside the normal course of their specified duties;

(B) in a manner inconsistent with the discharge of the responsibilities of such entity; or

(C) in contravention of the requirements, policies, and procedures required by this subsection.

(7) FEDERAL GOVERNMENT LIABILITY FOR VIOLATIONS OF THIS TITLE.—

(A) IN GENERAL.—If a Federal entity intentionally or willfully violates a provision of this title or a regulation promulgated under this title, the United States shall be liable to a person adversely affected by such violation in an amount equal to the sum of—

(i) the actual damages sustained by the person as a result of the violation or $1,000, whichever is greater; and

(ii) the costs of the action together with reasonable attorney fees as determined by the court.

(B) VENUE.—An action to enforce liability created under this subsection may be brought in the district court of the United States in—

(i) the district in which the complainant resides;

(ii) the district in which the principal place of business of the complainant is located;

(iii) the district in which the Federal entity that disclosed the information is located; or

(iv) the District of Columbia.

(C) STATUTE OF LIMITATIONS.—No action shall lie under this subsection unless such action is commenced not later than 2 years after the date of the violation that is the basis for the action.

(D) EXCLUSIVE CAUSE OF ACTION.—A cause of action under this subsection shall be the exclusive means available to a complainant seeking a remedy for a disclosure of information in violation of this title by a Federal entity.

SEC. 704. SHARING OF CLASSIFIED CYBERSECURITY THREAT INDICATORS.

(a) SHARING OF CLASSIFIED CYBERSECURITY THREAT INDICATORS.—The procedures established under section 702(a)(2) shall provide that classified cybersecurity threat indicators may only be—

(1) shared with certified entities;

(2) shared in a manner that is consistent with the need to protect the national security of the United States;

(3) shared with a person with an appropriate security clearance to receive such cybersecurity threat indicators; and

(4) used by a certified entity in a manner that protects such cybersecurity threat indicators from unauthorized disclosure.

(b) REQUIREMENT FOR GUIDELINES.—Not later than 60 days after the date of the enactment of this title, the Director of National Intelligence shall issue guidelines providing that appropriate Federal officials may, as the Director considers necessary to carry out this title—

(1) grant a security clearance on a temporary or permanent basis to an employee of a certified entity;

(2) grant a security clearance on a temporary or permanent basis to a certified entity and approval to use appropriate facilities; or

(3) expedite the security clearance process for such an employee or entity, if appropriate, in a manner consistent with the need to protect the national security of the United States.

(c) DISTRIBUTION OF PROCEDURES AND GUIDELINES.—Following the establishment of the procedures under section 702(a)(2) and the issuance of the guidelines under subsection (b), the Secretary and the Director of National Intelligence shall expeditiously distribute such procedures and guidelines to—

(1) appropriate governmental entities and private entities;

(2) the Committee on Armed Services, the Committee on Commerce, Science, and Transportation, the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, and the Select Committee on Intelligence of the Senate; and

(3) the Committee on Armed Services, the Committee on Energy and Commerce, the Committee on Homeland Security, the Committee on the Judiciary, and the Permanent Select Committee on Intelligence of the House of Representatives.

SEC. 705. LIMITATION ON LIABILITY AND GOOD FAITH DEFENSE FOR CYBERSECURITY ACTIVITIES.

(a) IN GENERAL.—No civil or criminal cause of action shall lie or be maintained in any Federal or State court against any entity acting as authorized by this title, and any such action shall be dismissed promptly for activities authorized by this title consisting of the voluntary disclosure of a lawfully obtained cybersecurity threat indicator—

(1) to a cybersecurity exchange pursuant to section 703(a);

(2) by a provider of cybersecurity services to a customer of that provider;

(3) to a private entity or governmental entity that provides or manages critical infrastructure (as that term is used in section 1016 of the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c)); or

(4) to any other private entity under section 701(a), if the cybersecurity threat indicator is also disclosed within a reasonable time to a cybersecurity exchange.

(b) GOOD FAITH DEFENSE.—If a civil or criminal cause of action is not barred under subsection (a), a reasonable good faith reliance that this title permitted the conduct complained of is a complete defense against any civil or criminal action brought under this title or any other law.

(c) LIMITATION ON USE OF CYBERSECURITY THREAT INDICATORS FOR REGULATORY ENFORCEMENT ACTIONS.—No Federal entity may use a cybersecurity threat indicator received pursuant to this title as evidence in a regulatory enforcement action against the entity that lawfully shared the cybersecurity threat indicator with a cybersecurity exchange that is a Federal entity.

(d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT, NATIONAL SECURITY, OR HOMELAND SECURITY PURPOSES.—No civil or criminal cause of action shall lie or be maintained in any Federal or State court against any entity, and any such action shall be dismissed promptly, for a failure to disclose a cybersecurity threat indicator if—

(1) the Attorney General or the Secretary determines that disclosure of a cybersecurity threat indicator would impede a civil or criminal investigation and submits a written request to delay notification for up to 30 days, except that the Attorney General or the Secretary may, by a subsequent written request, revoke such delay or extend the period of time set forth in the original request made under this paragraph if further delay is necessary; or

(2) the Secretary, the Attorney General, or the Director of National Intelligence determines that disclosure of a cybersecurity threat indicator would threaten national or homeland security and submits a written request to delay notification, except that the Secretary, the Attorney General, or the Director, may, by a subsequent written request, revoke such delay or extend the period of time set forth in the original request made under this paragraph if further delay is necessary.

(e) LIMITATION ON LIABILITY FOR FAILURE TO ACT.—No civil or criminal cause of action shall lie or be maintained in any Federal or State court against any private entity, or any officer, employee, or agent of such an entity, and any such action shall be dismissed promptly, for the reasonable failure to act on information received under this title.

(f) DEFENSE FOR BREACH OF CONTRACT.—Compliance with lawful restrictions placed on the disclosure or use of cybersecurity threat indicators is a complete defense to any tort or breach of contract claim originating in a failure to disclose cybersecurity threat indicators to a third party.

(g) LIMITATION ON LIABILITY PROTECTIONS.—Any person who, knowingly or acting in gross negligence, violates a provision of this title or a regulation promulgated under this title shall—

(1) not receive the protections of this title; and

(2) be subject to any criminal or civil cause of action that may arise under any other State or Federal law prohibiting the conduct in question.

SEC. 706. CONSTRUCTION AND FEDERAL PREEMPTION.

(a) CONSTRUCTION.—Nothing in this title may be construed—

(1) to limit any other existing authority or lawful requirement to monitor information systems and information that is stored on, processed by, or transiting such information systems, operate countermeasures, and retain, use or disclose lawfully obtained information;

(2) to permit the unauthorized disclosure of—

(A) information that has been determined by the Federal Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations;

(B) any restricted data (as that term is defined in paragraph (y) of section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014));

(C) information related to intelligence sources and methods; or

(D) information that is specifically subject to a court order or a certification, directive, or other authorization by the Attorney General precluding such disclosure;

(3) to provide additional authority to, or modify an existing authority of, the Department of Defense or the National Security Agency or any other element of the intelligence community to control, modify, require, or otherwise direct the cybersecurity efforts of a non-Federal entity or a Federal entity;

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

(5) to prohibit a new information sharing relationship;

(6) to require a new information sharing relationship between a Federal entity and a private entity;

(7) to limit the ability of a non-Federal entity or a Federal entity to receive data about its information systems, including lawfully obtained cybersecurity threat indicators;

(8) to authorize or prohibit any law enforcement, homeland security, or intelligence activities not otherwise authorized or prohibited under another provision of law;

(9) 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;

(10) to authorize or limit liability for actions that would violate the regulations adopted by the Federal Communications Commission on preserving the open Internet, or any successor regulations thereto, nor to modify or alter the obligations of private entities under such regulations; or

(11) to prevent a governmental entity from using information not acquired through a cybersecurity exchange for regulatory purposes.

(b) FEDERAL PREEMPTION.—This title supersedes any law or requirement of a State or political subdivision of a State that restricts or otherwise expressly regulates the provision of cybersecurity services or the acquisition, interception, retention, use or disclosure of communications, records, or other information by private entities to the extent such law contains requirements inconsistent with this title.

(c) PRESERVATION OF OTHER STATE LAW.—Except as expressly provided, nothing in this title shall be construed to preempt the applicability of any other State law or requirement.

(d) NO CREATION OF A RIGHT TO INFORMATION.—The provision of information to a non-Federal entity under this title does not create a right or benefit to similar information by any other non-Federal entity.

(e) PROHIBITION ON REQUIREMENT TO PROVIDE INFORMATION TO THE FEDERAL GOVERNMENT.—Nothing in this title may be construed to permit a Federal entity—

(1) to require a non-Federal entity to share information with the Federal Government;

(2) to condition the disclosure of unclassified or classified cybersecurity threat indicators pursuant to this title with a non-Federal entity on the provision of cybersecurity threat information to the Federal Government; or

(3) to condition the award of any Federal grant, contract or purchase on the provision of cybersecurity threat indicators to a Federal entity, if the provision of such indicators does not reasonably relate to the nature of activities, goods, or services covered by the award.

(f) LIMITATION ON USE OF INFORMATION.—No cybersecurity threat indicators obtained pursuant to this title may be used, retained, or disclosed by a Federal entity or non-Federal entity, except as authorized under this title.

(g) DECLASSIFICATION AND SHARING OF INFORMATION.—Consistent with the exemptions from public disclosure of section 704(d), the Director of National Intelligence, in consultation with the Secretary and the head of the Federal entity in possession of the information, shall facilitate the declassification and sharing of information in the possession of a Federal entity that is related to cybersecurity threats, as the Director deems appropriate.

(h) REPORT ON IMPLEMENTATION.—Not later than 2 years after the date of the enactment of this title, the Secretary, the Director of National Intelligence, the Attorney General, and the Secretary of Defense shall jointly submit to Congress a report that—

(1) describes the extent to which the authorities conferred by this title have enabled the Federal Government and the private sector to mitigate cybersecurity threats;

(2) discloses any significant acts of noncompliance by a non-Federal entity with this title, with special emphasis on privacy and civil liberties, and any measures taken by the Federal Government to uncover such noncompliance;

(3) describes in general terms the nature and quantity of information disclosed and received by governmental entities and private entities under this title; and

(4) identifies the emergence of new threats or technologies that challenge the adequacy of the law, including the definitions, authorities and requirements of this title, for keeping pace with the threat.

(i) REQUIREMENT FOR ANNUAL REPORT.—On an annual basis, the Director of National Intelligence shall provide a report to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives on the implementation of section 704. Such report, which shall be submitted in a classified and in an unclassified form, shall include a list of private entities that receive classified cybersecurity threat indicators under this title, except that the unclassified report shall not contain information that may be used to identify specific private entities unless such private entities consent to such identification.

SEC. 707. DEFINITIONS.

In this title:

(1) CERTIFIED ENTITY.—The term ''certified entity'' means a protected entity, a self-protected entity, or a provider of cybersecurity services that—

(A) possesses or is eligible to obtain a security clearance, as determined by the Director of National Intelligence; and

(B) is able to demonstrate to the Director of National Intelligence that such provider or such entity can appropriately protect and use classified cybersecurity threat indicators.

(2) CYBERSECURITY CRIME.—The term ''cybersecurity crime'' means the violation of a provision of State or Federal law relating to computer crimes, including a violation of any provision of title 18, United States Code, enacted or amended by the Computer Fraud and Abuse Act of 1986 (Public Law 99–474; 100 Stat. 1213).

(3) CYBERSECURITY EXCHANGE.—The term ''cybersecurity exchange'' means any governmental entity or private entity designated by the Secretary of Homeland Security, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, to receive and distribute cybersecurity threat indicators under section 703(a).

(4) CYBERSECURITY SERVICES.—The term ''cybersecurity services'' means products, goods, or services intended to detect, mitigate, or prevent cybersecurity threats.

(5) CYBERSECURITY THREAT.—The term ''cybersecurity threat'' means any action that may result in unauthorized access to, exfiltration of, manipulation of, harm of, or impairment to the integrity, confidentiality, or availability of an information system or information that is stored on, processed by, or transiting an information system, except that none of the following shall be considered a cybersecurity threat—

(A) actions protected by the first amendment to the Constitution of the United States; and

(B) exceeding authorized access of an information system, if such access solely involves a violation of consumer terms of service or consumer licensing agreements.

(6) CYBERSECURITY THREAT INDICATOR.—The term ''cybersecurity threat indicator'' means information—

(A) that is reasonably necessary to describe—

(i) malicious reconnaissance, including anomalous patterns of communications that reasonably appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

(ii) a method of defeating a technical control;

(iii) a technical vulnerability;

(iv) a method of defeating an operational control;

(v) 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 technical control or an operational control;

(vi) malicious cyber command and control;

(vii) the actual or potential harm caused by an incident, including information exfiltrated as a result of defeating a technical control or an operational control when it is necessary in order to identify or describe a cybersecurity threat;

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

(ix) any combination thereof; and

(B) from which reasonable efforts have been made to remove information that can be used to identify specific persons unrelated to the cybersecurity threat.

(7) FEDERAL CYBERSECURITY CENTER.—The term ''Federal cybersecurity center'' means the Department of Defense Cyber Crime Center, the Intelligence Community Incident Response Center, the United States Cyber Command Joint Operations Center, the National Cyber Investigative Joint Task Force, the National Security Agency/Central Security Service Threat Operations Center, the United States Computer Emergency Readiness Team, or successors to such centers.

(8) FEDERAL ENTITY.—The term ''Federal entity'' means an agency or department of the United States, or any component, officer, employee, or agent of such an agency or department.

(9) GOVERNMENTAL ENTITY.—The term ''governmental entity'' means any Federal entity and agency or department of a State, local, tribal, or territorial government other than an educational institution, or any component, officer, employee, or agent of such an agency or department.

(10) INFORMATION SYSTEM.—The term ''information system'' means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, including communications with, or commands to, specialized systems such as industrial and process control systems, telephone switching and private branch exchanges, and environmental control systems.

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

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

(13) MONITOR.—The term ''monitor'' means the interception, acquisition, or collection of information that is stored on, processed by, or transiting an information system for the purpose of identifying cybersecurity threats.

(14) NON-FEDERAL ENTITY.—The term ''non-Federal entity'' means a private entity or a governmental entity other than a Federal entity.

(15) OPERATIONAL CONTROL.—The term ''operational control'' means a security control for an information system that primarily is implemented and executed by people.

(16) PRIVATE ENTITY.—The term ''private entity'' has the meaning given the term ''person'' in section 1 of title 1, United States Code, and does not include a governmental entity.

(17) PROTECT.—The term ''protect'' means actions undertaken to secure, defend, or reduce the vulnerabilities of an information system, mitigate cybersecurity threats, or otherwise enhance information security or

the resiliency of information systems or assets.

(18) TECHNICAL CONTROL.—The term ''technical control'' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that system.

(19) TECHNICAL VULNERABILITY.—The term ''technical vulnerability'' means any attribute of hardware or software that could enable or facilitate the defeat of a technical control.

(20) THIRD PARTY.—The term ''third party'' includes Federal entities and non-Federal entities.

SA 2704. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 10, strike lines 16 through 25 and insert the following:

and the member agencies; and

(2) ensure the timely implementation of decisions of the Council.

(d) PRESIDENTIAL AUTHORITY.—The Chairperson may take emergency action to fulfill the responsibilities of the Council if—

(1) the Chairperson determines that the emergency action is necessary to prevent or mitigate an imminent cybersecurity threat; and

(2) the President approves the emergency action.

SA 2705. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 153, strike lines 17 through 20 and insert the following:

Not later than 1 year after the date of enactment of this Act, the Secretary of Energy, in consultation with the Secretary, the Secretary of Defense, the Director of National Intelligence, the Director of the National Institute of Standards and Technology, the Federal Energy Regulatory Commission, and the Electric Reliability Organization (as defined in section 215(a) of the Federal Power Act (16 U.S.C. 824o(a)) shall submit to Congress a report on—

SA 2706. Mrs. MURRAY submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 11, strike lines 12 and 13 and insert the following:

as appropriate;

(7) the National Guard Bureau; and

(8) the Department.

At the end of title IV, add the following:

SEC. 416. REPORT ON ROLES AND MISSIONS OF THE NATIONAL GUARD IN STATE STATUS IN SUPPORT OF THE CYBERSECURITY EFFORTS OF THE FEDERAL GOVERNMENT.

(a) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall, in consultation with the Secretary of Defense and the Chief of the National Guard Bureau, submit to the appropriate committees of Congress a report on the roles and missions of the National Guard in State status (commonly referred to as ''title 32 status'') in support of the cybersecurity efforts of the Department of Homeland Security, the Department of Defense, and other departments and agencies of the Federal Government.

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

(1) A description of the current roles and missions of the National Guard in State status in support of the cybersecurity efforts of the Federal Government, and a description of the policies and authorities governing the discharge of such roles and missions.

(2) A description of potential roles and missions for the National Guard in State status in support of the cybersecurity efforts of the Federal Government, a description of the policies and authorities to govern the discharge of such roles and missions, and recommendations for such legislative or administrative actions as may be required to establish and implement such roles and missions.

(3) An assessment of the feasability and advisability of public-private partnerships on homeland cybersecurity missions involving the National Guard in State status, including the advisability of using pilot programs to evaluate feasability and advisability of such partnerships.

(c) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term ''appropriate committees of Congress'' means—

(1) the Committee on Homeland Security and Governmental Affairs and the Committee on Armed Services of the Senate; and

(2) the Committee on Homeland Security and the Committee on Armed Services of the House of Representatives.

SA 2707. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 34, strike lines 3 through 17 and insert the following:

(1) provide a Federal agency with additional or greater authority for regulating the security of critical cyber infrastructure than any authority the Federal agency has under other law;

(2) limit or restrict the authority of the Department, or any other Federal agency, under any other provision of law; or

(3) permit any owner (including a certified

SA 2708. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 182, strike lines 7 through 16 and insert the following:

(d) PROTECTION OF INFORMATION FROM DISCLOSURE.—A cybersecurity threat indicator or any other information that was developed, submitted, obtained, or shared in connection with the implementation of this section shall be—

(1) exempt from disclosure under section 552(b)(3) of title 5, United States Code;

(2) exempt from disclosure under any State, local, or tribal law or regulation that requires public disclosure of information or records by a public or quasi-public entity; and

(3) treated as voluntarily shared information under section 552 of title 5, United States Code, or any comparable State, local, or tribal law or regulation.

SA 2709. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States, which was ordered to lie on the table; as follows:

On page 23, strike line 18 and all that follows through page 25, line 8.

SA 2710. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States, which was ordered to lie on the table; as follows:

On page 20, strike line 6 and all that follows through page 22, line 14, and insert the following:

date on which the top-level assessment is completed under section 102(a)(2)(A), each sector coordinating council shall propose to the Council voluntary outcome-based cybersecurity practices (referred to in this section as ''cybersecurity practices'') sufficient to effectively remediate or mitigate cyber risks identified through an assessment conducted under section 102(a) comprised of—

(1) industry best practices, standards, and guidelines; or

(2) practices developed by the sector coordinating council in coordination with owners and operators, voluntary consensus standards development organizations, representatives of State and local governments, the private sector, and appropriate information sharing and analysis organizations.

(b) REVIEW OF CYBERSECURITY PRACTICES.—

(1) IN GENERAL.—The Council shall, in consultation with owners and operators, the Critical Infrastructure Partnership Advisory Council, and appropriate information sharing and analysis organizations, and in coordination with appropriate representatives from State and local governments—

(A) consult with relevant security experts and institutions of higher education, including university information security centers, appropriate nongovernmental cybersecurity experts, and representatives from national laboratories;

(B) review relevant regulations or compulsory standards or guidelines;

(C) review cybersecurity practices proposed under subsection (a); and

(D) consider any amendments to the cybersecurity practices and any additional cybersecurity practices necessary to ensure adequate remediation or mitigation of the cyber risks identified through an assessment conducted under section 102(a).

(2) ADOPTION.—

(A) IN GENERAL.—Not later than 1 year after the date on which the top-level assessment is completed under section 102(a)(2)(A), the Council shall—

(i) adopt any cybersecurity practices proposed under subsection (a) that adequately remediate or mitigate identified cyber risks and any associated consequences identified through an assessment conducted under section 102(a); and

(ii) adopt any amended or additional cybersecurity practices necessary to ensure the adequate remediation or mitigation of the cyber risks identified through an assessment conducted under section 102(a).

(B) NO SUBMISSION BY SECTOR COORDINATING COUNCIL.—If a sector coordinating council fails to propose to the Council cybersecurity practices under subsection (a) within 180 days of the date on which the top-level assessment is completed under section

102(a)(2)(A), not later than 1 year after the date on which the top-level assessment is completed under section 102(a)(2)(A) the Council shall adopt cybersecurity

---

SA 2711. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States, which was ordered to lie on the table; as follows:

On page 43, beginning on line 14, strike ''section 104(c)(1) and section 106'' and insert the following: ''sections 104(c)(1), 106, and 704(d)''.

SA 2712. Ms. CANTWELL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States, which was ordered to lie on the table; as follows:

On page 41, strike line 5 and all that follows through page 42, line 4, and insert the following:

date on which the Council completes the adoption of cybersecurity practices under section 103(b)(2), and every year thereafter, the Council shall submit to the appropriate congressional committees a report on the effectiveness of this title in reducing the risk of cyber attack to critical infrastructure.

(b) CONTENTS.—Each report submitted under subsection (a) shall include—

(1) a discussion of cyber risks and associated consequences and whether the cybersecurity practices developed under section 103 are sufficient to effectively remediate and mitigate cyber risks and associated consequences; and

(2) an analysis of—

(A) whether owners of critical cyber infrastructure are successfully implementing the cybersecurity practices adopted under section 103;

(B) whether the critical infrastructure of the United States is effectively secured from cybersecurity threats, vulnerabilities, and consequences; and

(C) whether additional legislative authority

SA 2713. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States, which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

TITLE ____—CYBER ATTACKS INVOLVING DRONES

SEC. __01. DEFINITIONS.

In this title—

(1) the term ''drone'' means any aerial vehicle that—

(A) does not carry a human operator;

(B) uses aerodynamic or aerostatic forces to provide vehicle lift;

(C) can fly autonomously or be piloted remotely;

(D) can be expendable or recoverable; and

(E) can carry a lethal or nonlethal payload; and

(2) the term ''law enforcement party'' means a person or entity authorized by law, or funded, in whole or in part, by the Government of the United States, to investigate or prosecute offenses against the United States.

SEC. __02. PROTECTION AGAINST UNAUTHORIZED USE OF DRONES.

(a) IN GENERAL.—No drone may be deployed or otherwise used by any officer, employee, or contractor of the Federal Government or by a person or entity acting under the authority of, or funded in whole or in part by, the Government of the United States, until the National Cybersecurity Council or other person, division, or entity placed in charge of cybersecurity efforts in the United States certifies that any such drone is immune from a cyber attack or other compromise of control, navigation, or data.

(b) EMPLOYMENT OF CERTIFIED DRONES.—Except as provided in section __03, no officer, employee, or contractor of the Federal Government or any person or entity acting under the authority of, or funded in whole or in part by, the Government of the United States shall use a drone to gather evidence or other information pertaining to criminal conduct or conduct in violation of a statute or regulation, except to the extent authorized in a warrant that satisfies the requirements of the Fourth Amendment to the Constitution of the United States.

SEC. __03. EXCEPTIONS.

This title does not prohibit any of the following:

(1) PATROL OF BORDERS.—The use of a drone certified under section __02(a) to patrol national borders to prevent or deter illegal entry of any persons or illegal substances.

(2) EXIGENT CIRCUMSTANCES.—The use of a drone certified under section __02(a) by a law enforcement party when exigent circumstances exist. For the purposes of this paragraph, exigent circumstances exist when the law enforcement party possesses reasonable suspicion that under particular circumstances, swift action to prevent imminent danger to life is necessary.

(3) HIGH RISK.—The use of a drone certified under section __02(a) to counter a high risk of a terrorist attack by a specific individual or organization, when the Secretary of Homeland Security determines credible intelligence indicates there is such a risk.

SEC. __04. REMEDIES FOR VIOLATION.

Any aggrieved party may in a civil action obtain all appropriate relief to prevent or remedy a violation of this title.

SEC. __05. PROHIBITION ON USE OF EVIDENCE.

No evidence obtained or collected in violation of this title may be admissible as evidence in a criminal prosecution in any court of law in the United States.

SA 2714. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 23, strike line 19 and all that follows through page 34, line 19, and insert the following:

(1) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide a Federal agency that has authority for regulating the security of critical cyber infrastructure any authority in addition to or to a greater extent than the authority the Federal agency has under other law.

(2) AVOIDANCE OF CONFLICT.—No cybersecurity practice shall—

(A) prevent an owner (including a certified owner) from complying with any law or regulation; or

(B) require an owner (including a certified owner) to implement cybersecurity measures that prevent the owner from complying with any law or regulation.

(3) AVOIDANCE OF DUPLICATION.—Where regulations or compulsory standards regulate the security of critical cyber infrastructure, a cybersecurity practice shall, to the greatest extent possible, complement or otherwise improve the regulations or compulsory standards.

(h) INDEPENDENT REVIEW.—

(1) IN GENERAL.—Each cybersecurity practice shall be publicly reviewed by the relevant sector coordinating council and the Critical Infrastructure Partnership Advisory Council, which may include input from relevant institutions of higher education, including university information security centers, national laboratories, and appropriate non-governmental cybersecurity experts.

(2) CONSIDERATION BY COUNCIL.—The Council shall consider any review conducted under paragraph (1).

(i) VOLUNTARY TECHNICAL ASSISTANCE.—At the request of an owner or operator of critical infrastructure, the Council shall provide guidance on the application of cybersecurity practices to the critical infrastructure.

SEC. 104. VOLUNTARY CYBERSECURITY PROGRAM FOR CRITICAL INFRASTRUCTURE.

(a) VOLUNTARY CYBERSECURITY PROGRAM FOR CRITICAL INFRASTRUCTURE.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Council, in consultation with owners and operators and the Critical Infrastructure Partnership Advisory Council, shall establish the Voluntary Cybersecurity Program for Critical Infrastructure in accordance with this section.

(2) ELIGIBILITY.—

(A) IN GENERAL.—An owner of critical cyber infrastructure may apply for certification under the Voluntary Cybersecurity Program for Critical Infrastructure.

(B) CRITERIA.—The Council shall establish criteria for owners of critical infrastructure that is not critical cyber infrastructure to be eligible to apply for certification in the Voluntary Cybersecurity Program for Critical Infrastructure.

(3) APPLICATION FOR CERTIFICATION.—An owner of critical cyber infrastructure or an owner of critical infrastructure that meets the criteria established under paragraph (2)(B) that applies for certification under this subsection shall—

(A) select and implement cybersecurity measures of their choosing that satisfy the outcome-based cybersecurity practices established under section 103; and

(B)(i) certify in writing and under penalty of perjury to the Council that the owner has developed and effectively implemented cybersecurity measures sufficient to satisfy the outcome-based cybersecurity practices established under section 103; or

(ii) submit to the Council an assessment verifying that the owner has developed and effectively implemented cybersecurity measures sufficient to satisfy the outcome-based cybersecurity practices established under section 103.

(4) CERTIFICATION.—Upon receipt of a self-certification under paragraph (3)(B)(i) or an assessment under paragraph (3)(B)(ii) the Council shall certify an owner.

(5) NONPERFORMANCE.—If the Council determines that a certified owner is not in compliance with the cybersecurity practices established under section 103, the Council shall—

(A) notify the certified owner of such determination; and

(B) work with the certified owner to remediate promptly any deficiencies.

(6) REVOCATION.—If a certified owner fails to remediate promptly any deficiencies identified by the Council, the Council shall revoke the certification of the certified owner.

(7) REDRESS.—

(A) IN GENERAL.—If the Council revokes a certification under paragraph (6), the Council shall—

(i) notify the owner of such revocation; and

(ii) provide the owner with specific cybersecurity measures that, if implemented, would remediate any deficiencies.

(B) RECERTIFICATION.—If the Council determines that an owner has remedied any deficiencies and is in compliance with the cybersecurity practices, the Council may recertify the owner.

(b) ASSESSMENTS.—

(1) THIRD-PARTY ASSESSMENTS.—The Council, in consultation with owners and operators and the Critical Infrastructure Protection Advisory Council, shall enter into agreements with qualified third-party private entities, to conduct assessments that use reliable, repeatable, performance-based evaluations and metrics to assess whether an owner certified under subsection (a)(3)(B)(ii) is in compliance with all applicable cybersecurity practices.

(2) TRAINING.—The Council shall ensure that third party assessors described in paragraph (1) undergo regular training and accreditation.

(3) OTHER ASSESSMENTS.—Using the procedures developed under this section, the Council may perform cybersecurity assessments of a certified owner based on actual knowledge or a reasonable suspicion that the certified owner is not in compliance with the cybersecurity practices or any other risk-based factors as identified by the Council.

(4) NOTIFICATION.—The Council shall provide copies of any assessments by the Federal Government to the certified owner.

(5) ACCESS TO INFORMATION.—

(A) IN GENERAL.—For the purposes of an assessment conducted under this subsection, a certified owner shall provide the Council, or a third party assessor, any reasonable access necessary to complete an assessment.

(B) PROTECTION OF INFORMATION.—Information provided to the Council, the Council's designee, or any assessor during the course of an assessment under this section shall be protected from disclosure in accordance with section 106.

(c) BENEFITS OF CERTIFICATION.—

(1) LIMITATIONS ON CIVIL LIABILITY.—

(A) IN GENERAL.—In any civil action for damages directly caused by an incident related to a cyber risk identified through an assessment conducted under section 102(a), a certified owner shall not be liable for any punitive damages intended to punish or deter if the certified owner is in substantial compliance with the appropriate cybersecurity practices at the time of the incident related to that cyber risk.

(B) LIMITATION.—Subaragraph (A) shall only apply to harm directly caused by the incident related to the cyber risk and shall not apply to damages caused by any additional or intervening acts or omissions by the owner.

(2) EXPEDITED SECURITY CLEARANCE PROCESS.—The Council, in coordination with the Office of the Director of National Intelligence, shall establish a procedure to expedite the provision of security clearances to appropriate personnel employed by a certified owner.

(3) PRIORITIZED TECHNICAL ASSISTANCE.—The Council shall ensure that certified owners are eligible to receive prioritized technical assistance.

(4) PROVISION OF CYBER THREAT INFORMATION.—The Council shall develop, in coordination with certified owners, a procedure for ensuring that certified owners are, to the maximum extent practicable and consistent with the protection of sources and methods, informed of relevant real-time cyber threat information.

(5) PUBLIC RECOGNITION.—With the approval of a certified owner, the Council may publicly recognize the certified owner if the Council determines such recognition does not pose a risk to the security of critical cyber infrastructure.

(6) STUDY TO EXAMINE BENEFITS OF PROCUREMENT PREFERENCE.—

(A) IN GENERAL.—The Federal Acquisition Regulatory Council, in coordination with the Council and with input from relevant private sector individuals and entities, shall conduct a study examining the potential benefits of establishing a procurement preference for the Federal Government for certified owners.

(B) AREAS.—The study under subparagraph (A) shall include a review of—

(i) potential persons and related property and services that could be eligible for preferential consideration in the procurement process;

(ii) development and management of an approved list of categories of property and services that could be eligible for preferential consideration in the procurement process;

(iii) appropriate mechanisms to implement preferential consideration in the procurement process, including—

(I) establishing a policy encouraging Federal agencies to conduct market research and industry outreach to identify property and services that adhere to relevant cybersecurity practices;

(II) authorizing the use of a mark for the Voluntary Cybersecurity Program for Critical Infrastructure to be used for marketing property or services to the Federal Government;

(III) establishing a policy of encouraging procurement of certain property and services from an approved list;

(IV) authorizing the use of a preference by Federal agencies in the evaluation process; and

(V) authorizing a requirement in certain solicitations that the person providing the property or services be a certified owner; and

(iv) benefits of and impact on the economy and efficiency of the Federal procurement system, if preferential consideration were given in the procurement process to encourage the procurement of property and services that adhere to relevant baseline performance goals establishing under the Voluntary Cybersecurity Program for Critical Infrastructure.

SEC. 105. RULES OF CONSTRUCTION.

Nothing in this title shall be construed to—

(1) provide additional authority for any sector-specific agency or any Federal agency that is not a sector-specific agency with responsibilities for regulating the security of critical infrastructure to establish standards or other cybersecurity measures that are applicable to the security of critical infrastructure not otherwise authorized by law;

(2) limit or restrict the authority of the Department, or any other Federal agency, under any other provision of law; or

(3) permit any owner (including a certified owner) to fail to comply with any other law or regulation, unless specifically authorized.

(h) NO LIMITATION ON CONTRACTUAL LIABILITY.—No limitation on liability or good faith defense provided under this section shall apply to any civil claim against a private entity arising under contract law.

SA 2715. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 199, between lines 12 and 13, insert the following:

SA 2716. Mr. LEE submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. DISTRICT OF COLUMBIA PAIN-CAPABLE UNBORN CHILD PROTECTION ACT.

(a) SHORT TITLE.—This section may be cited as the ''District of Columbia Pain-Capable Unborn Child Protection Act''.

(b) LEGISLATIVE FINDINGS.—Congress finds and declares the following:

(1) Pain receptors (nociceptors) are present throughout the unborn child's entire body and nerves link these receptors to the brain's thalamus and subcortical plate by no later than 20 weeks after fertilization.

(2) By 8 weeks after fertilization, the unborn child reacts to touch. After 20 weeks, the unborn child reacts to stimuli that would be recognized as painful if applied to an adult human, for example, by recoiling.

(3) In the unborn child, application of such painful stimuli is associated with significant increases in stress hormones known as the stress response.

(4) Subjection to such painful stimuli is associated with long-term harmful neurodevelopmental effects, such as altered pain sensitivity and, possibly, emotional, behavioral, and learning disabilities later in life.

(5) For the purposes of surgery on unborn children, fetal anesthesia is routinely administered and is associated with a decrease in stress hormones compared to their level when painful stimuli are applied without such anesthesia.

(6) The position, asserted by some medical experts, that the unborn child is incapable of experiencing pain until a point later in pregnancy than 20 weeks after fertilization predominately rests on the assumption that the ability to experience pain depends on the cerebral cortex and requires nerve connections between the thalamus and the cortex. However, recent medical research and analysis, especially since 2007, provides strong evidence for the conclusion that a functioning cortex is not necessary to experience pain.

(7) Substantial evidence indicates that children born missing the bulk of the cerebral cortex, those with hydranencephaly, nevertheless experience pain.

(8) In adult humans and in animals, stimulation or ablation of the cerebral cortex does not alter pain perception, while stimulation or ablation of the thalamus does.

(9) Substantial evidence indicates that structures used for pain processing in early development differ from those of adults, using different neural elements available at specific times during development, such as the subcortical plate, to fulfill the role of pain processing.

(10) The position, asserted by some commentators, that the unborn child remains in a coma-like sleep state that precludes the unborn child experiencing pain is inconsistent with the documented reaction of unborn children to painful stimuli and with the experience of fetal surgeons who have found it necessary to sedate the unborn child with anesthesia to prevent the unborn child from

engaging in vigorous movement in reaction to invasive surgery.

(11) Consequently, there is substantial medical evidence that an unborn child is capable of experiencing pain at least by 20 weeks after fertilization, if not earlier.

(12) It is the purpose of the Congress to assert a compelling governmental interest in protecting the lives of unborn children from the stage at which substantial medical evidence indicates that they are capable of feeling pain.

(13) The compelling governmental interest in protecting the lives of unborn children from the stage at which substantial medical evidence indicates that they are capable of feeling pain is intended to be separate from and independent of the compelling governmental interest in protecting the lives of unborn children from the stage of viability, and neither governmental interest is intended to replace the other.

(14) The District Council of the District of Columbia, operating under authority delegated by Congress, repealed all limitations on abortion at any stage of pregnancy, effective April 29, 2004.

(15) Article I, section 8 of the Constitution of the United States of America provides that the Congress shall ''exercise exclusive Legislation in all Cases whatsoever'' over the District established as the seat of government of the United States, now known as the District of Columbia. The constitutional responsibility for the protection of pain-capable unborn children within the Federal District resides with the Congress.

(c) DISTRICT OF COLUMBIA PAIN-CAPABLE UNBORN CHILD PROTECTION.—

(1) IN GENERAL.—Chapter 74 of title 18, United States Code, is amended by inserting after section 1531 the following:

''§ 1532. District of Columbia pain-capable unborn child protection

''(a) UNLAWFUL CONDUCT.—Notwithstanding any other provision of law, including any legislation of the District of Columbia under authority delegated by Congress, it shall be unlawful for any person to perform an abortion within the District of Columbia, or attempt to do so, unless in conformity with the requirements set forth in subsection (b).

''(b) REQUIREMENTS FOR ABORTIONS.—

''(1) The physician performing or attempting the abortion shall first make a determination of the probable post-fertilization age of the unborn child or reasonably rely upon such a determination made by another physician. In making such a determination, the physician shall make such inquiries of the pregnant woman and perform or cause to be performed such medical examinations and tests as a reasonably prudent physician, knowledgeable about the case and the medical conditions involved, would consider necessary to make an accurate determination of post-fertilization age.

''(2)(A) Except as provided in subparagraph (B), the abortion shall not be performed or attempted, if the probable post-fertilization age, as determined under paragraph (1), of the unborn child is 20 weeks or greater.

''(B) Subject to subparagraph (C), subparagraph (A) does not apply if, in reasonable medical judgment, the abortion is necessary to save the life of a pregnant woman whose life is endangered by a physical disorder, physical illness, or physical injury, including a life-endangering physical condition caused by or arising from the pregnancy itself, but not including psychological or emotional conditions or any claim or diagnosis that the woman will engage in conduct which she intends to result in her death.

''(C) A physician terminating or attempting to terminate a pregnancy under the exception provided by subparagraph (B) may do so only in the manner which, in reasonable medical judgment, provides the best opportunity for the unborn child to survive, unless, in reasonable medical judgment, termination of the pregnancy in that manner would pose a greater risk of—

''(i) the death of the pregnant woman; or

''(ii) the substantial and irreversible physical impairment of a major bodily function, not including psychological or emotional conditions, of the pregnant woman;

than would other available methods.

''(c) CRIMINAL PENALTY.—Whoever violates subsection (a) shall be fined under this title or imprisoned for not more than 2 years, or both.

''(d) BAR TO PROSECUTION.—A woman upon whom an abortion in violation of subsection (a) is performed or attempted may not be prosecuted under, or for a conspiracy to violate, subsection (a), or for an offense under section 2, 3, or 4 based on such a violation.

''(e) CIVIL REMEDIES.—

''(1) CIVIL ACTION BY WOMAN ON WHOM THE ABORTION IS PERFORMED.—A woman upon whom an abortion has been performed or attempted in violation of subsection (a), may in a civil action against any person who engaged in the violation obtain appropriate relief.

''(2) CIVIL ACTION BY RELATIVES.—The father of an unborn child who is the subject of an abortion performed or attempted in violation of subsection (a), or a maternal grandparent of the unborn child if the pregnant woman is an unemancipated minor, may in a civil action against any person who engaged in the violation, obtain appropriate relief, unless the pregnancy resulted from the plaintiff's criminal conduct or the plaintiff consented to the abortion.

''(3) APPROPRIATE RELIEF.—Appropriate relief in a civil action under this subsection includes—

''(A) objectively verifiable money damages for all injuries, psychological and physical, occasioned by the violation of this section;

''(B) statutory damages equal to three times the cost of the abortion; and

''(C) punitive damages.

''(4) INJUNCTIVE RELIEF.—

''(A) IN GENERAL.—A qualified plaintiff may in a civil action obtain injunctive relief to prevent an abortion provider from performing or attempting further abortions in violation of this section.

''(B) DEFINITION.—In this paragraph the term 'qualified plaintiff' means—

''(i) a woman upon whom an abortion is performed or attempted in violation of this section;

''(ii) any person who is the spouse, parent, sibling or guardian of, or a current or former licensed health care provider of, that woman; or

''(iii) the United States Attorney for the District of Columbia.

''(5) ATTORNEYS FEES FOR PLAINTIFF.—The court shall award a reasonable attorney's fee as part of the costs to a prevailing plaintiff in a civil action under this subsection.

''(6) ATTORNEYS FEES FOR DEFENDANT.—If a defendant in a civil action under this section prevails and the court finds that the plaintiff's suit was frivolous and brought in bad faith, the court shall also render judgment for a reasonable attorney's fee in favor of the defendant against the plaintiff.

''(7) AWARDS AGAINST WOMAN.—Except under paragraph (6), in a civil action under this subsection, no damages, attorney's fee or other monetary relief may be assessed against the woman upon whom the abortion was performed or attempted.

''(f) PROTECTION OF PRIVACY IN COURT PROCEEDINGS.—

''(1) IN GENERAL.—Except to the extent the Constitution or other similarly compelling reason requires, in every civil or criminal action under this section, the court shall make such orders as are necessary to protect the anonymity of any woman upon whom an abortion has been performed or attempted if she does not give her written consent to such disclosure. Such orders may be made upon motion, but shall be made sua sponte if not otherwise sought by a party.

''(2) ORDERS TO PARTIES, WITNESSES, AND COUNSEL.—The court shall issue appropriate orders under paragraph (1) to the parties, witnesses, and counsel and shall direct the sealing of the record and exclusion of individuals from courtrooms or hearing rooms to the extent necessary to safeguard her identity from public disclosure. Each such order shall be accompanied by specific written findings explaining why the anonymity of the woman must be preserved from public disclosure, why the order is essential to that end, how the order is narrowly tailored to serve that interest, and why no reasonable less restrictive alternative exists.

''(3) PSEUDONYM REQUIRED.—In the absence of written consent of the woman upon whom an abortion has been performed or attempted, any party, other than a public official, who brings an action under paragraphs (1), (2), or (4) of subsection (e) shall do so under a pseudonym.

''(4) LIMITATION.—This subsection shall not be construed to conceal the identity of the plaintiff or of witnesses from the defendant or from attorneys for the defendant.

''(g) REPORTING.—

''(1) DUTY TO REPORT.—Any physician who performs or attempts an abortion within the District of Columbia shall report that abortion to the relevant District of Columbia health agency (hereinafter in this section referred to as the 'health agency') on a schedule and in accordance with forms and regulations prescribed by the health agency.

''(2) CONTENTS OF REPORT.—The report shall include the following:

''(A) POST-FERTILIZATION AGE.—For the determination of probable postfertilization age of the unborn child, whether ultrasound was employed in making the determination, and the week of probable post-fertilization age that was determined.

''(B) METHOD OF ABORTION.—Which of the following methods or combination of methods was employed:

''(i) Dilation, dismemberment, and evacuation of fetal parts also known as 'dilation and evacuation'.

''(ii) Intra-amniotic instillation of saline, urea, or other substance (specify substance) to kill the unborn child, followed by induction of labor.

''(iii) Intracardiac or other intra-fetal injection of digoxin, potassium chloride, or other substance (specify substance) intended to kill the unborn child, followed by induction of labor.

''(iv) Partial-birth abortion, as defined in section 1531.

''(v) Manual vacuum aspiration without other methods.

''(vi) Electrical vacuum aspiration without other methods.

''(vii) Abortion induced by use of mifepristone in combination with misoprostol; or

''(viii) if none of the methods described in the other clauses of this subparagraph was employed, whatever method was employed.

''(C) AGE OF WOMAN.—The age or approximate age of the pregnant woman.

''(D) COMPLIANCE WITH REQUIREMENTS FOR EXCEPTION.—The facts relied upon and the basis for any determinations required to establish compliance with the requirements

for the exception provided by subsection (b)(2).

''(3) EXCLUSIONS FROM REPORTS.—

''(A) A report required under this subsection shall not contain the name or the address of the woman whose pregnancy was terminated, nor shall the report contain any other information identifying the woman.

''(B) Such report shall contain a unique Medical Record Number, to enable matching the report to the woman's medical records.

''(C) Such reports shall be maintained in strict confidence by the health agency, shall not be available for public inspection, and shall not be made available except—

''(i) to the United States Attorney for the District of Columbia or that Attorney's delegate for a criminal investigation or a civil investigation of conduct that may violate this section; or

''(ii) pursuant to court order in an action under subsection (e).

''(4) PUBLIC REPORT.—Not later than June 30 of each year beginning after the date of enactment of this paragraph, the health agency shall issue a public report providing statistics for the previous calendar year compiled from all of the reports made to the health agency under this subsection for that year for each of the items listed in paragraph (2). The report shall also provide the statistics for all previous calendar years during which this section was in effect, adjusted to reflect any additional information from late or corrected reports. The health agency shall take care to ensure that none of the information included in the public reports could reasonably lead to the identification of any pregnant woman upon whom an abortion was performed or attempted.

''(5) FAILURE TO SUBMIT REPORT.—

''(A) LATE FEE.—Any physician who fails to submit a report not later than 30 days after the date that report is due shall be subject to a late fee of $1,000 for each additional 30-day period or portion of a 30-day period the report is overdue.

''(B) COURT ORDER TO COMPLY.—A court of competent jurisdiction may, in a civil action commenced by the health agency, direct any physician whose report under this subsection is still not filed as required, or is incomplete, more than 180 days after the date the report was due, to comply with the requirements of this section under penalty of civil contempt.

''(C) DISCIPLINARY ACTION.—Intentional or reckless failure by any physician to comply with any requirement of this subsection, other than late filing of a report, constitutes sufficient cause for any disciplinary sanction which the Health Professional Licensing Administration of the District of Columbia determines is appropriate, including suspension or revocation of any license granted by the Administration.

''(6) FORMS AND REGULATIONS.—Not later than 90 days after the date of the enactment of this section, the health agency shall prescribe forms and regulations to assist in compliance with this subsection.

''(7) EFFECTIVE DATE OF REQUIREMENT.—Paragraph (1) of this subsection takes effect with respect to all abortions performed on and after the first day of the first calendar month beginning after the effective date of such forms and regulations.

''(h) DEFINITIONS.—In this section the following definitions apply:

''(1) ABORTION.—The term 'abortion' means the use or prescription of any instrument, medicine, drug, or any other substance or device—

''(A) to intentionally kill the unborn child of a woman known to be pregnant; or

''(B) to otherwise intentionally terminate the pregnancy of a woman known to be pregnant with an intention other than to increase the probability of a live birth, to preserve the life or health of the child after live birth, or to remove a dead unborn child who died as the result of natural causes in utero, accidental trauma, or a criminal assault on the pregnant woman or her unborn child, and which causes the premature termination of the pregnancy.

''(2) ATTEMPT AN ABORTION.—The term 'attempt', with respect to an abortion, means conduct that, under the circumstances as the actor believes them to be, constitutes a substantial step in a course of conduct planned to culminate in performing an abortion in the District of Columbia.

''(3) FERTILIZATION.—The term 'fertilization' means the fusion of human spermatozoon with a human ovum.

''(4) HEALTH AGENCY.—The term 'health agency' means the Department of Health of the District of Columbia or any successor agency responsible for the regulation of medical practice.

''(5) PERFORM.—The term 'perform', with respect to an abortion, includes induce an abortion through a medical or chemical intervention including writing a prescription for a drug or device intended to result in an abortion.

''(6) PHYSICIAN.—The term 'physician' means a person licensed to practice medicine and surgery or osteopathic medicine and surgery, or otherwise licensed to legally perform an abortion.

''(7) POST-FERTILIZATION AGE.—The term 'post-fertilization age' means the age of the unborn child as calculated from the fusion of a human spermatozoon with a human ovum.

''(8) PROBABLE POST-FERTILIZATION AGE OF THE UNBORN CHILD.—The term 'probable postfertilization age of the unborn child' means what, in reasonable medical judgment, will with reasonable probability be the postfertilization age of the unborn child at the time the abortion is planned to be performed or induced.

''(9) REASONABLE MEDICAL JUDGMENT.—The term 'reasonable medical judgment' means a medical judgment that would be made by a reasonably prudent physician, knowledgeable about the case and the treatment possibilities with respect to the medical conditions involved.

''(10) UNBORN CHILD.—The term 'unborn child' means an individual organism of the species homo sapiens, beginning at fertilization, until the point of being born alive as defined in section 8(b) of title 1.

''(11) UNEMANCIPATED MINOR.—The term 'unemancipated minor' means a minor who is subject to the control, authority, and supervision of a parent or guardian, as determined under the law of the State in which the minor resides.

''(12) WOMAN.—The term 'woman' means a female human being whether or not she has reached the age of majority.''.

(2) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 74 of title 18, United States Code, is amended by adding at the end the following new item:

''1532. District of Columbia pain-capable unborn child protection.''.

(3) CHAPTER HEADING AMENDMENTS.—

(A) CHAPTER HEADING IN CHAPTER.—The chapter heading for chapter 74 of title 18, United States Code, is amended by striking ''**PARTIAL BIRTH ABORTIONS**'' and inserting ''**ABORTIONS**''.

(B) TABLE OF CHAPTERS FOR PART I.—The item relating to chapter 74 in the table of chapters at the beginning of part I of title 18, United States Code, is amended by striking ''**PARTIAL BIRTH ABORTIONS**'' and inserting ''**ABORTIONS**''.

SA 2717. Mrs. SHAHEEN submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 121, beginning on line 16, strike ''summer enrichment programs, to be provided by nonprofit organizations, in math, computer programming'' and insert ''summer enrichment programs and programs offered before or after normal school hours, to be provided by nonprofit organizations, in math, computer science, computer programming''.

On page 125, line 12, insert '', such as mentors from private sector entities'' after ''appropriate''.

SA 2718. Mrs. SHAHEEN submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title VI, add the following:

SEC. 606. COOPERATION WITH NATO ON CYBER DEFENSE.

(a) FINDINGS.—Congress makes the following findings:

(1) The November 2010 NATO Lisbon Summit Declaration asserts, ''Cyber threats are rapidly increasing and evolving in sophistication. In order to ensure NATO's permanent and unfettered access to cyberspace and integrity of its critical systems, we will take into account the cyber dimension of modern conflicts in NATO's doctrine and improve its capabilities to detect, assess, prevent, defend and recover in case of a cyber-attack against systems of critical importance to the Alliance.''

(2) In an April 2012 speech, Secretary of State Hillary Clinton stated, ''There is a steady drumbeat of [cyber] attacks on governments, on businesses, on all kinds of networks every single day. And we have to be in a position to protect ourselves and, under Article 5, protect our NATO partners. There have been some rather significant attacks on NATO partners over the last several years that have caused consternation because of the damage done to classified information, and so therefore we are in the process of working toward a joint capability.''

(b) SENSE OF CONGRESS.—It is the sense of Congress that it is in the interest of the United States to continue to work with NATO members, partners, and allies to develop the necessary cyber capabilities, including prevention, detection, recovery, and response, to deter aggression and prevent coercion through the cyber domain.

(c) CONGRESSIONAL BRIEFING.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of State, after consultation with the heads of relevant Federal agencies, shall brief Congress on—

(A) the ability of NATO to detect, assess, prevent, defend, and recover from cyber attacks to its critical systems, networks, and other combat equipment;

(B) implementation of the NATO Policy on Cyber Defense;

(C) development of NATO's Computer Incident Response Capability;

(D) development and contributions of NATO's Cooperative Cyber Defense Center of Excellence; and

(E) NATO cooperation with other international organizations, including the European Union, the Council of Europe, the United Nations, and the Organization for the Security and Co-operation in Europe.

(2) CONTRIBUTIONS FROM RELEVANT FEDERAL AGENCIES.—Not later than 30 days before the

date on which the briefing is to be provided under paragraph (1), the Secretary of State, in coordination with the Secretary of Defense, shall consult with and obtain information relevant to the briefing from the head of each relevant Federal agency.

(3) PERIODIC UPDATES.—The Secretary of State shall provide periodic briefings to Congress to highlight significant developments relating to the issues described in paragraph (1).

SA 2719. Mr. KOHL (for himself, Mr. WHITEHOUSE, and Mr. COONS) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE __—ECONOMIC ESPIONAGE PENALTY ENHANCEMENT

SEC. __01. SHORT TITLE.

This title may be cited as the ''Economic Espionage Penalty Enhancement Act of 2012''.

SEC. __02. PROTECTING U.S. BUSINESSES FROM FOREIGN ESPIONAGE.

(a) FOR OFFENSES COMMITTED BY INDIVIDUALS.—Section 1831(a) of title 18, United States Code, is amended in the matter following paragraph (5)—

(1) by striking ''15 years'' and inserting ''20 years''; and

(2) by striking ''not more than $500,000'' and inserting ''not more than $5,000,000''.

(b) FOR OFFENSES COMMITTED BY ORGANIZATIONS.—Section 1831(b) of title 18, United States Code, is amended by striking ''not more than $10,000,000'' and inserting ''not more than the greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided''.

SEC. __03. REVIEW BY THE UNITED STATES SENTENCING COMMISSION.

(a) IN GENERAL.—Pursuant to its authority under section 994(p) of title 28, United States Code, the United States Sentencing Commission shall review and, if appropriate, amend the Federal sentencing guidelines and policy statements applicable to persons convicted of offenses relating to the transmission or attempted transmission of a stolen trade secret outside of the United States or economic espionage, in order to reflect the intent of Congress that penalties for such offenses under the Federal sentencing guidelines and policy statements appropriately reflect the seriousness of these offenses, account for the potential and actual harm caused by these offenses, and provide adequate deterrence against such offenses.

(b) REQUIREMENTS.—In carrying out this section, the United States Sentencing Commission shall—

(1) consider the extent to which the Federal sentencing guidelines and policy statements appropriately account for the simple misappropriation of a trade secret, including the sufficiency of the existing enhancement for these offenses to address the seriousness of this conduct;

(2) consider whether additional enhancements in the Federal sentencing guidelines and policy statements are appropriate to account for—

(A) the transmission or attempted transmission of a stolen trade secret outside of the United States; and

(B) the transmission or attempted transmission of a stolen trade secret outside of the United States that is committed or attempted to be committed for the benefit of a foreign government, foreign instrumentality, or foreign agent;

(3) ensure the Federal sentencing guidelines and policy statements reflect the seriousness of these offenses and the need to deter such conduct;

(4) ensure reasonable consistency with other relevant directives, Federal sentencing guidelines and policy statements, and related Federal statutes;

(5) make any necessary conforming changes to the Federal sentencing guidelines and policy statements; and

(6) ensure that the Federal sentencing guidelines adequately meet the purposes of sentencing as set forth in section 3553(a)(2) of title 18, United States Code.

(c) CONSULTATION.—In carrying out the review required under this section, the Commission shall consult with individuals or groups representing law enforcement, owners of trade secrets, victims of economic espionage offenses, the Department of Justice, the Department of State, the Department of Homeland Security, and the Office of the United States Trade Representative.

(d) REVIEW.—Not later than 180 days after the date of enactment of this title, the Commission shall complete its consideration and review under this section.

SA 2720. Mrs. MCCASKILL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 106, line 15, insert '', the Director of the Office of Management and Budget,'' after ''the Secretary''.

On page 110, line 8, strike ''to the extent practicable,''.

On page 115, line 22, strike '', to the extent practicable,''.

SA 2721. Mrs. MCCASKILL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. PERFORMANCE OF CYBERSECURITY AUTHORITIES BY GOVERNMENT EMPLOYEES.

(a) CYBERSECURITY FUNCTIONS.—Section 5(2) of the Federal Activities Inventory Reform Act of 1998 (Public Law 105–270; 31 U.S.C. 501 note) is amended—

(1) by redesignating subparagraph (C) as subparagraph (D); and

(2) by inserting after subparagraph (B) the following:

''(C) CYBERSECURITY FUNCTIONS INCLUDED.—The term includes any authority provided to the Federal Government under title I, II, V, or VII, or an amendment made by title I, II, V, or VII, of the Cybersecurity Act of 2012 that is not explicitly authorized to be performed by a non-Federal individual or entity.''.

(b) CLARIFICATION OF PROHIBITION ON CONTRACTORS PERFORMING INHERENTLY GOVERNMENTAL FUNCTIONS.—The Federal Activities Inventory Reform Act of 1998 (Public Law 105–270; 31 U.S.C. 501 note) is amended by inserting after section 2 the following:

''SEC. 2A. PROHIBITION ON CONTRACTORS PERFORMING INHERENTLY GOVERNMENTAL FUNCTIONS.

''The head of an executive agency or employee of an executive agency may not enter into a contract or any other agreement under which an individual or entity that is not an employee of the Federal Government performs an inherently governmental function.''.

SA 2722. Mrs. MCCASKILL submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 137, strike line 6 and all that follows through page 139, line 15, and insert the following:

SEC. 408. RECRUITMENT AND RETENTION PROGRAM FOR THE NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS.

(a) IN GENERAL.—Subtitle E of title II of the Homeland Security Act of 2002, as added by section 204, is amended by adding at the end the following:

''SEC. 245. RECRUITMENT AND RETENTION PROGRAM FOR THE NATIONAL CENTER FOR CYBERSECURITY AND COMMUNICATIONS.

SA 2723. Mr. PRYOR submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title IV, add the following:

SEC. 416. GAO STUDY AND REPORT ON SMALL BUSINESS CYBERSECURITY ISSUES.

(a) STUDY.—The Comptroller General of the United States shall conduct a study identifying—

(1) small business cybersecurity concerns;

(2) existing efforts by Federal agencies having responsibility to assist small businesses with cybersecurity issues (including the Department of Homeland Security, the Federal Trade Commission, the Small Business Administration, and the National Institute of Standards and Technology) to raise small business awareness of cybersecurity issues; and

(3) ways the Federal agencies described in paragraph (2) plan to improve small business awareness of and preparedness for cybersecurity issues.

(b) REPORT.—Not later than 18 months after the date of enactment of this Act, the Comptroller General shall submit to Congress a report containing—

(1) the results of the study conducted under subsection (a); and

(2) recommendations, if any, based on the results of the study conducted under subsection (a).

SA 2724. Ms. MIKULSKI submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Strike section 404 and insert the following:

SEC. 404. FEDERAL CYBER SCHOLARSHIP-FOR-SERVICE PROGRAM.

(a) IN GENERAL.—The Director of the National Science Foundation, in coordination with the Secretary and the Director of the Office of Personnel Management, shall carry out a Federal Cyber Scholarship-for-Service program—

(1) to increase the capacity of institutions of higher education to produce cybersecurity professionals; and

(2) to recruit and train the next generation of information technology professionals, industry control security professionals, and security managers to meet the needs of the cybersecurity mission for the Federal Government and State, local, and tribal governments.

(b) PROGRAM DESCRIPTION AND COMPONENTS.—The program carried out under subsection (a) shall—

(1) incorporate findings from the assessment and development of the strategy under section 405;

(2) provide institutions of higher education, including community colleges, with sufficient funding to carry out a scholarship program, as described in subsection (c); and

(3) provide assistance to institutions of higher education in establishing or expanding educational opportunities and resources in cybersecurity, as authorized under section 5 of the Cyber Security Research and Development Act (15 U.S.C. 7404).

(c) SCHOLARSHIP PROGRAM.—

(1) INSTITUTIONS OF HIGHER EDUCATION.—An institution of higher education that carries out a scholarship program under subsection (b)(2) shall—

(A) provide 2- or 3-year scholarships to students who are enrolled in a program of study at the institution of higher education leading to a degree, credential, or specialized program certification in the cybersecurity field, in an amount that covers each student's tuition and fees at the institution and provides the student with an additional stipend;

(B) require each scholarship recipient, as a condition of receiving a scholarship under the program—

(i) to enter into an agreement under which the recipient agrees to work in the cybersecurity mission of a Federal, State, local, or tribal agency for a period equal to the length of the scholarship following receipt of the student's degree, credential, or specialized program certification; and

(ii) to refund any scholarship payments received by the recipient, in accordance with rules established by the Director of the National Science Foundation, in coordination with the Secretary, if a recipient does not meet the terms of the scholarship program; and

(C) provide clearly documented evidence of a strong existing program in cybersecurity, which may include designation as a Center of Academic Excellence in Information Assurance Education by the National Security Agency and the Department of Homeland Security.

(2) SCHOLARSHIP ELIGIBILITY.—To be eligible to receive a scholarship under a scholarship program carried out by an institution of higher education under subsection (b)(2), an individual shall—

(A) be a full-time student of the institution of higher education who is likely to receive a baccalaureate degree, a masters degree, or a research-based doctoral degree during the 3-year period beginning on the date on which the individual receives the scholarship;

(B) be a citizen of lawful permanent resident of the United States;

(C) demonstrate a commitment to a career in improving the security of information infrastructure; and

(D) have demonstrated a high level of proficiency in fields relevant to the cybersecurity profession, which may include mathematics, engineering, business, public policy, social sciences, law, or computer sciences.

(3) OTHER PROGRAM REQUIREMENTS.—The Director of the National Science Foundation, in coordination with the Secretary and the Director of the Office of Personnel Management, shall ensure that each scholarship program carried out under subsection (b)(2)—

(A) provides a procedure by which the National Science Foundation or a Federal agency may, consistent with regulations of the Office of Personnel Management, request and fund security clearances for scholarships recipients, including providing for clearances during summer internships and after the recipient receives the degree, credential, or specialized program certification; and

(B) provides opportunities for students to receive temporary appointments for meaningful employment in the cybersecurity mission of a Federal agency during vacation periods and for internships.

(4) HIRING AUTHORITY.—

(A) IN GENERAL.—For purposes of any law or regulation governing the appointment of individuals in the Federal civil service, upon receiving a degree for which an individual received a scholarship under a scholarship program carried out by an institution of higher education under subsection (b)(2), the individual shall be—

(i) hired under the authority provided for in section 213.3102(r) or title 5, Code of Federal Regulations; and

(ii) exempt from competitive service.

(B) COMPETITIVE SERVICE POSITION.—Upon satisfactory fulfillment of the service term of an individual hired under subparagraph (A), the individual may be converted to a competitive service position with competition if the individual meets the requirements for that position.

(5) EVALUATION AND REPORT.—The Director of the National Science Foundation shall evaluate and report periodically to Congress on—

(A) the success of any scholarship programs carried out under subsection (b)(2) in recruiting individuals for scholarships; and

(B) hiring and retaining individuals who receive scholarships under a scholarship program carried out under subsection (b)(2) in the public sector workforce.

(d) BENCHMARKS.—

(1) PROPOSALS.—A proposal submitted to the Director of the National Science Foundation for assistance under subsection (b)(3) shall include—

(A) clearly stated goals translated into a set of expected measurable outcomes that can be monitored; and

(B) an evaluation plan that explains how the outcomes described in subparagraph (A) will be measured.

(2) USE OF GOALS.—The Director of the National Science Foundation shall use the goals included in a proposal submitted under paragraph (1)—

(A) to track the progress of a recipient of assistance under subsection (b)(3);

(B) to guide a project carried out using assistance under subsection (b)(3); and

(C) to evaluate the impact of a project carried out using assistance under subsection (b)(3).

SA 2725. Mr. LEE submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. TO CLASSIFY THE INDIVIDUAL MANDATE AS A NON-TAX.

(a) FINDING.—Congress finds that on June 28, 2012, the Supreme Court ruled that the individual mandate imposed by section 1501 of the Patient Protection and Affordable Care Act (Public Law 111–148) and amended by section 10106 of such Act and sections 1002 and 1004 of the Health Care and Education Reconciliation Act of 2010 (Public Law 111–152), has certain functional characteristics of a tax and could be sustained as an exercise of Congress's power to tax under article I, section 8, clause 1 of the Constitution.

(b) CLASSIFICATION OF INDIVIDUAL MANDATE AS NON-TAX.—

(1) IN GENERAL.—Section 1501 of the Patient Protection and Affordable Care Act (Public Law 111–148) is amended by adding at the end the following new subsection:

''(e) RULE OF CONSTRUCTION.—Nothing in the amendments made by this section shall be construed as imposing any tax or as an exercise of any power of Congress enumerated in article I, section 8, clause 1 of, or the 16th amendment to, the Constitution.''.

(2) EFFECTIVE DATE.—The amendment made by this section shall apply as if included in the enactment of section 1501 of the Patient Protection and Affordable Care Act.

SA 2726. Mr. PRYOR submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 119, between lines 14 and 15, insert the following:

(b) GEOGRAPHIC DISPERSION.—In establishing academic and professional Centers of Excellence in cybersecurity under this section, the Secretary and the Secretary of Defense shall consider the need to avoid undue geographic concentration among any one category of States based on their predominant rural or urban character as indicated by population density.

SA 2727. Mr. BLUMENTHAL (for himself, Mr. SCHUMER, Ms. KLOBUCHAR, Mr. WYDEN, Mr. AKAKA, Mr. SANDERS, and Mrs. SHAHEEN) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. PROHIBITED ACTIVITY.

(a) IN GENERAL.—Section 1030(a) of title 18, United States Code, is amended—

(1) in paragraph (7)(C), by inserting ''or'' after the semicolon; and

(2) by inserting after paragraph (7)(C) the following:

''(8) acting as an employer, knowingly and intentionally—

''(A) for the purposes of employing, promoting, or terminating employment, compels or coerces any person to authorize access, such as by providing a password or similar information through which a computer may be accessed, to a protected computer that is not the employer's protected computer, and thereby obtains information from such protected computer; or

''(B) discharges, disciplines, discriminates against in any manner, or threatens to take any such action against, any person—

''(i) for failing to authorize access described in subparagraph (A) to a protected computer that is not the employer's protected computer; or

''(ii) who has filed any complaint or instituted or caused to be instituted any proceeding under or related to this paragraph, or has testified or is about to testify in any such proceeding;''.

(b) FINE.—Section 1030(c) of title 18, United States Code, is amended—

(1) in paragraph (4)(G)(ii), by striking the period at the end and inserting ''; and''; and

(2) by adding at the end the following:

''(5) a fine under this title, in the case of an offense under subsection (a)(8) or an attempt to commit an offense punishable under this paragraph.''.

(c) DEFINITIONS.—Section 1030(e) of title 18, United States Code, is amended—

(1) in paragraph (11), by striking ''and'' after the semicolon;

(2) in paragraph (12), by striking the period and inserting a semicolon; and

(3) by adding at the end the following:

''(13) the term 'employee' means an employee, as such term is defined in section 201(2) of the Genetic Information Nondiscrimination Act of 2008 (42 U.S.C. 2000ff(2));

''(14) the term 'employer' means an employer, as such term is defined in such section 201(2); and

''(15) the term 'employer's protected computer' means a protected computer of the employer, including any protected computer owned, operated, or otherwise controlled by, for, or on behalf of that employer.''.

(d) EXCEPTIONS.—Section 1030(f) of title 18, United States Code, is amended—

(1) by striking ''(f) This'' and inserting ''(f)(1) This''; and

(2) by adding at the end the following:

''(2)(A) Nothing in subsection (a)(8) shall be construed to limit the authority of a court of competent jurisdiction to grant equitable relief in a civil action, if the court determines that there are specific and articulable facts showing that there are reasonable grounds to believe that the information sought to be obtained is relevant and material to protecting the intellectual property, a trade secret, or confidential business information of the party seeking the relief.

''(B) Notwithstanding subsection (a)(8), the prohibition in such subsection shall not apply to an employer's actions if—

''(i) the employer discharges or otherwise disciplines an individual for good cause and an activity protected under subsection (a)(8) is not a motivating factor for the discharge or discipline of the individual;

''(ii) a State enacts a law that specifically waives subsection (a)(8) with respect to a particular class of State government employees or employees who work with individuals under 13 years of age, and the employer's action relates to an employee in such class; or

''(iii) an Executive agency (as defined in section 105 of title 5), a military department (as defined in section 102 of such title), or any other entity within the executive branch that comes into the possession of classified information, including the Defense Intelligence Agency, National Security Agency, and National Reconnaissance Office, specifically waives subsection (a)(8) with respect to a particular class of employees requiring eligibility for access to classified information under Executive Order 12968 (60 Fed. Reg. 40245), or any successor thereto, and the employer's action relates to an employee in such class.''.

SA 2728. Mr. BLUMENTHAL submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 192, strike line 19, and all that follows through page 193, line 22, and insert the following:

(i) the actual damages sustained by the person as a result of the violation or $50,000, whichever is greater; and

(ii) the costs of the action together with reasonable attorney fees as determined by the court.

(B) VENUE.—An action to enforce liability created under this subsection may be brought in the district court of the United States in—

(i) the district in which the complainant resides;

(ii) the district in which the principal place of business of the complainant is located;

(iii) the district in which the Federal entity that disclosed the information is located; or

(iv) the District of Columbia.

(C) STATUTE OF LIMITATIONS.—No action shall lie under this subsection unless such action is commenced not later than 2 years after the date of the violation that is the basis for the action.

(h) CRIMINAL PENALTIES.—A person who knowingly violates a provision of this title shall be—

(1) for each such violation, fined not more than $50,000, imprisoned for not more than 1 year, or both;

(2) for each such violation committed under false pretenses, fined not more than $100,000, imprisoned for not more than 5 years, or both; and

(3) for each such violation committed for commercial advantage, personal gain, or malicious harm, fined not more than $250,000, imprisoned for not more than 10 years, or both.

SA 2729. Mr. WARNER (for himself and Ms. SNOWE) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 138, line 2, after ''subsection (a)'' insert '', including guidelines that provide for interoperable, non-proprietary technologies wherever possible''.

SA 2730. Mr. THUNE submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 134, line 4, insert ''and in consultation with Centers of Academic Excellence in Information Assurance Education designated by the National Security Agency and the Department,'' after ''United States Code,''.

SA 2731. Mr. REID (for Mr. LIEBERMAN (for himself, Ms. COLLINS, Mr. ROCKEFELLER, Mrs. FEINSTEIN, and Mr. CARPER)) proposed an amendment to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; as follows:

On page 20, strike line 3 and all that follows through page 42, line 10, and insert the following:

SEC. 103. VOLUNTARY CYBERSECURITY PRACTICES.

(a) PRIVATE SECTOR DEVELOPMENT OF CYBERSECURITY PRACTICES.—Not later than 180 days after the date of enactment of this Act, each sector coordinating council shall propose to the Council voluntary outcome-based cybersecurity practices (referred to in this section as ''cybersecurity practices'') sufficient to effectively remediate or mitigate cyber risks identified through an assessment conducted under section 102(a) comprised of—

(1) industry best practices, standards, and guidelines; or

(2) practices developed by the sector coordinating council in coordination with owners and operators, voluntary consensus standards development organizations, representatives of State and local governments, the private sector, and appropriate information sharing and analysis organizations.

(b) REVIEW OF CYBERSECURITY PRACTICES.—

(1) IN GENERAL.—The Council shall, in consultation with owners and operators, the Critical Infrastructure Partnership Advisory Council, and appropriate information sharing and analysis organizations, and in coordination with appropriate representatives from State and local governments—

(A) consult with relevant security experts and institutions of higher education, including university information security centers, appropriate nongovernmental cybersecurity experts, and representatives from national laboratories;

(B) review relevant regulations or compulsory standards or guidelines;

(C) review cybersecurity practices proposed under subsection (a); and

(D) consider any amendments to the cybersecurity practices and any additional cybersecurity practices necessary to ensure adequate remediation or mitigation of the cyber risks identified through an assessment conducted under section 102(a).

(2) ADOPTION.—

(A) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Council shall—

(i) adopt any cybersecurity practices proposed under subsection (a) that adequately remediate or mitigate identified cyber risks and any associated consequences identified through an assessment conducted under section 102(a); and

(ii) adopt any amended or additional cybersecurity practices necessary to ensure the adequate remediation or mitigation of the cyber risks identified through an assessment conducted under section 102(a).

(B) NO SUBMISSION BY SECTOR COORDINATING COUNCIL.—If a sector coordinating council fails to propose to the Council cybersecurity practices under subsection (a) within 180 days of the date of enactment of this Act, not later than 1 year after the date of enactment of this Act the Council shall adopt cybersecurity practices that adequately remediate or mitigate identified cyber risks and associated consequences identified through an assessment conducted under section 102(a) for the sector.

(c) FLEXIBILITY OF CYBERSECURITY PRACTICES.—Each sector coordinating council and the Council shall periodically assess cybersecurity practices, but not less frequently than once every 3 years, and update or modify cybersecurity practices as necessary to ensure adequate remediation and mitigation of the cyber risks identified through an assessment conducted under section 102(a).

(d) PRIORITIZATION.—Based on the risk assessments performed under section 102(a), the Council shall prioritize the development of cybersecurity practices to ensure the reduction or mitigation of the greatest cyber risks.

(e) PRIVATE SECTOR RECOMMENDED MEASURES.—Each sector coordinating council shall develop voluntary recommended cybersecurity measures that provide owners reasonable and cost-effective methods of meeting any cybersecurity practice.

(f) TECHNOLOGY NEUTRALITY.—No cybersecurity practice shall require—

(1) the use of a specific commercial information technology product; or

(2) that a particular commercial information technology product be designed, developed, or manufactured in a particular manner.

(g) RELATIONSHIP TO EXISTING REGULATIONS.—

(1) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to increase, decrease, or otherwise alter the existing authority of any Federal agency to regulate the security of critical cyber infrastructure.

(2) AVOIDANCE OF CONFLICT.—No cybersecurity practice shall—

(A) prevent an owner (including a certified owner) or operator from complying with any law or regulation; or

(B) require an owner (including a certified owner) or operator to implement cybersecurity measures that prevent the owner or operator from complying with any law or regulation.

(h) INDEPENDENT REVIEW.—

(1) IN GENERAL.—Each cybersecurity practice shall be publicly reviewed by the relevant sector coordinating council and the Critical Infrastructure Partnership Advisory Council, which may include input from relevant institutions of higher education, including university information security centers, national laboratories, and appropriate non-governmental cybersecurity experts.

(2) CONSIDERATION BY COUNCIL.—The Council shall consider any review conducted under paragraph (1).

(i) VOLUNTARY TECHNICAL ASSISTANCE.—At the request of an owner or operator of critical infrastructure, the Council shall provide guidance on the application of cybersecurity practices to the critical infrastructure.

SEC. 104. VOLUNTARY CYBERSECURITY PROGRAM FOR CRITICAL INFRASTRUCTURE.

(a) VOLUNTARY CYBERSECURITY PROGRAM FOR CRITICAL INFRASTRUCTURE.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Council, in consultation with owners and operators and the Critical Infrastructure Partnership Advisory Council, shall establish the Voluntary Cybersecurity Program for Critical Infrastructure in accordance with this section.

(2) ELIGIBILITY.—

(A) IN GENERAL.—An owner of critical cyber infrastructure may apply for certification under the Voluntary Cybersecurity Program for Critical Infrastructure.

(B) CRITERIA.—The Council shall establish criteria for owners of critical infrastructure that is not critical cyber infrastructure to be eligible to apply for certification in the Voluntary Cybersecurity Program for Critical Infrastructure.

(3) APPLICATION FOR CERTIFICATION.—An owner of critical cyber infrastructure or an owner of critical infrastructure that meets the criteria established under paragraph (2)(B) that applies for certification under this subsection shall—

(A) select and implement cybersecurity measures of their choosing that satisfy the outcome-based cybersecurity practices established under section 103; and

(B)(i) certify in writing and under penalty of perjury to the Council that the owner has developed and effectively implemented cybersecurity measures sufficient to satisfy the outcome-based cybersecurity practices established under section 103; or

(ii) submit to the Council an assessment verifying that the owner has developed and effectively implemented cybersecurity measures sufficient to satisfy the outcome-based cybersecurity practices established under section 103.

(4) CERTIFICATION.—Upon receipt of a self-certification under paragraph (3)(B)(i) or an assessment under paragraph (3)(B)(ii) the Council shall certify an owner.

(5) NONPERFORMANCE.—If the Council determines that a certified owner is not in compliance with the cybersecurity practices established under section 103, the Council shall—

(A) notify the certified owner of such determination; and

(B) work with the certified owner to remediate promptly any deficiencies.

(6) REVOCATION.—If a certified owner fails to remediate promptly any deficiencies identified by the Council, the Council shall revoke the certification of the certified owner.

(7) REDRESS.—

(A) IN GENERAL.—If the Council revokes a certification under paragraph (6), the Council shall—

(i) notify the owner of such revocation; and

(ii) provide the owner with specific cybersecurity measures that, if implemented, would remediate any deficiencies.

(B) RECERTIFICATION.—If the Council determines that an owner has remedied any deficiencies and is in compliance with the cybersecurity practices, the Council may recertify the owner.

(b) ASSESSMENTS.—

(1) THIRD-PARTY ASSESSMENTS.—The Council, in consultation with owners and operators and the Critical Infrastructure Protection Advisory Council, shall enter into agreements with qualified third-party private entities, to conduct assessments that use reliable, repeatable, performance-based evaluations and metrics to assess whether an owner certified under subsection (a)(3)(B)(ii) is in compliance with all applicable cybersecurity practices.

(2) TRAINING.—The Council shall ensure that third party assessors described in paragraph (1) undergo regular training and accreditation.

(3) OTHER ASSESSMENTS.—Using the procedures developed under this section, the Council may perform cybersecurity assessments of a certified owner based on actual knowledge or a reasonable suspicion that the certified owner is not in compliance with the cybersecurity practices or any other risk-based factors as identified by the Council.

(4) NOTIFICATION.—The Council shall provide copies of any assessments by the Federal Government to the certified owner.

(5) ACCESS TO INFORMATION.—

(A) IN GENERAL.—For the purposes of an assessment conducted under this subsection, a certified owner shall provide the Council, or a third party assessor, any reasonable access necessary to complete an assessment.

(B) PROTECTION OF INFORMATION.—Information provided to the Council, the Council's designee, or any assessor during the course of an assessment under this section shall be protected from disclosure in accordance with section 106.

(c) BENEFITS OF CERTIFICATION.—

(1) LIMITATIONS ON CIVIL LIABILITY.—

(A) IN GENERAL.—In any civil action for damages directly caused by an incident related to a cyber risk identified through an assessment conducted under section 102(a), a certified owner shall not be liable for any punitive damages intended to punish or deter if the certified owner is in substantial compliance with the appropriate cybersecurity practices at the time of the incident related to that cyber risk.

(B) LIMITATION.—Subaragraph (A) shall only apply to harm directly caused by the incident related to the cyber risk and shall not apply to damages caused by any additional or intervening acts or omissions by the owner.

(2) EXPEDITED SECURITY CLEARANCE PROCESS.—The Council, in coordination with the Office of the Director of National Intelligence, shall establish a procedure to expedite the provision of security clearances to appropriate personnel employed by a certified owner.

(3) PRIORITIZED TECHNICAL ASSISTANCE.—The Council shall ensure that certified owners are eligible to receive prioritized technical assistance.

(4) PROVISION OF CYBER THREAT INFORMATION.—The Council shall develop, in coordination with certified owners, a procedure for ensuring that certified owners are, to the maximum extent practicable and consistent with the protection of sources and methods, informed of relevant real-time cyber threat information.

(5) PUBLIC RECOGNITION.—With the approval of a certified owner, the Council may publicly recognize the certified owner if the Council determines such recognition does not pose a risk to the security of critical cyber infrastructure.

(6) STUDY TO EXAMINE BENEFITS OF PROCUREMENT PREFERENCE.—

(A) IN GENERAL.—The Federal Acquisition Regulatory Council, in coordination with the Council and with input from relevant private sector individuals and entities, shall conduct a study examining the potential benefits of establishing a procurement preference for the Federal Government for certified owners.

(B) AREAS.—The study under subparagraph (A) shall include a review of—

(i) potential persons and related property and services that could be eligible for preferential consideration in the procurement process;

(ii) development and management of an approved list of categories of property and services that could be eligible for preferential consideration in the procurement process;

(iii) appropriate mechanisms to implement preferential consideration in the procurement process, including—

(I) establishing a policy encouraging Federal agencies to conduct market research and industry outreach to identify property and services that adhere to relevant cybersecurity practices;

(II) authorizing the use of a mark for the Voluntary Cybersecurity Program for Critical Infrastructure to be used for marketing property or services to the Federal Government;

(III) establishing a policy of encouraging procurement of certain property and services from an approved list;

(IV) authorizing the use of a preference by Federal agencies in the evaluation process; and

(V) authorizing a requirement in certain solicitations that the person providing the property or services be a certified owner; and

(iv) benefits of and impact on the economy and efficiency of the Federal procurement system, if preferential consideration were given in the procurement process to encourage the procurement of property and services that adhere to relevant baseline performance goals establishing under the Voluntary Cybersecurity Program for Critical Infrastructure.

SEC. 105. RULES OF CONSTRUCTION.

Nothing in this title shall be construed to—

(1) provide additional authority for any sector-specific agency or any Federal agency that is not a sector-specific agency with responsibilities for regulating the security of critical infrastructure to establish standards or other cybersecurity measures that are applicable to the security of critical infrastructure not otherwise authorized by law;

(2) limit or restrict the authority of the Department, or any other Federal agency, under any other provision of law; or

(3) permit any owner (including a certified owner) to fail to comply with any other law or regulation, unless specifically authorized.

SEC. 106. PROTECTION OF INFORMATION.

(a) DEFINITIONS.—In this section—

(1) the term ''covered information'' means any information—

(A) submitted as part of the process established under section 102(a)(3);

(B) submitted under section 102(b)(2)(C);

(C) required to be submitted by owners under section 102(b)(4);

(D) provided to the Secretary, the Secretary's designee, or any assessor during the course of an assessment under section 104; or

(E) provided to the Secretary or the Inspector General of the Department through the tip line or another secure channel established under subsection (c); and

(2) the term ''Inspector General'' means an Inspector General described in subparagraph (A), (B), or (I) of section 11(b)(1) of the Inspector General Act of 1978 (5 U.S.C. App.), the Inspector General of the United States Postal Service, the Inspector General of the Central Intelligence Agency, and the Inspector General of the Intelligence Community.

(b) CRITICAL INFRASTRUCTURE INFORMATION.—

(1) IN GENERAL.—Covered information shall be treated as voluntarily shared critical infrastructure information under section 214 of the Homeland Security Act of 2002 (6 U.S.C. 133), except that the requirement of such section 214 that the information be voluntarily submitted shall not be required for protection of information under this section to apply.

(2) SAVINGS CLAUSE FOR EXISTING WHISTLEBLOWER PROTECTIONS.—With respect to covered information, the rights and protections relating to disclosure by individuals of voluntarily shared critical infrastructure information submitted under subtitle B of title II of the Homeland Security Act of 2002 (6 U.S.C. 131 et seq.) shall apply with respect to disclosure of the covered information by individuals.

(c) CRITICAL INFRASTRUCTURE CYBER SECURITY TIP LINE.—

(1) IN GENERAL.—The Secretary shall establish and publicize the availability of a Critical Infrastructure Cyber Security Tip Line (and any other secure means the Secretary determines would be desirable to establish), by which individuals may report—

(A) concerns involving the security of covered critical infrastructure against cyber risks; and

(B) concerns (in addition to any concerns described under subparagraph (A)) with respect to programs and functions authorized or funded under this title involving—

(i) a possible violation of any law, rule, regulation or guideline;

(ii) mismanagement;

(iii) risk to public health, safety, security, or privacy; or

(iv) other misfeasance or nonfeasance.

(2) DESIGNATION OF EMPLOYEES.—The Secretary and the Inspector General of the Department shall each designate employees authorized to receive concerns reported under this subsection that include—

(A) disclosure of covered information; or

(B) any other disclosure of information that is specifically prohibited by law or is specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs.

(3) HANDLING OF CERTAIN CONCERNS.—A concern described in paragraph (1)(B)—

(A) shall be received initially to the Inspector General of the Department;

(B) shall not be provided initially to the Secretary; and

(C) may be provided to the Secretary if determined appropriate by the Inspector General of the Department.

(d) RULES OF CONSTRUCTION.—Nothing in this section shall be construed to—

(1) limit or otherwise affect the right, ability, duty, or obligation of any entity to use or disclose any information of that entity, including in the conduct of any judicial or other proceeding;

(2) prevent the classification of information submitted under this section if that information meets the standards for classification under Executive Order 12958, or any successor thereto, or affect measures and controls relating to the protection of classified information as prescribed by Federal statute or under Executive Order 12958, or any successor thereto;

(3) limit or otherwise affect the ability of an entity, agency, or authority of a State, a local government, or the Federal Government or any other individual or entity under applicable law to obtain information that is not covered information (including any information lawfully and properly disclosed generally or broadly to the public) and to use such information in any manner permitted by law, including the disclosure of such information under—

(A) section 552 or 2302(b)(8) of title 5, United States Code;

(B) section 2409 of title 10, United States Code; or

(C) any other Federal, State, or local law, ordinance, or regulation that protects against retaliation an individual who discloses information that the individual reasonably believes evidences a violation of any law, rule, or regulation, gross mismanagement, substantial and specific danger to public health, safety, or security, or other misfeasance or nonfeasance;

(4) prevent the Secretary from using information required to be submitted under this Act for enforcement of this title, including enforcement proceedings subject to appropriate safeguards;

(5) authorize information to be withheld from any committee of Congress, the Comptroller General, or any Inspector General;

(6) affect protections afforded to trade secrets under any other provision of law; or

(7) create a private right of action for enforcement of any provision of this section.

(e) AUDIT.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Inspector General of the Department shall conduct an audit of the management of covered information under this title and report the findings to appropriate congressional committees.

(2) CONTENTS.—The audit under paragraph (1) shall include assessments of—

(A) whether the covered information is adequately safeguarded against inappropriate disclosure;

(B) the processes for marking and disseminating the covered information and resolving any disputes;

(C) how the covered information is used for the purposes of this title, and whether that use is effective;

(D) whether sharing of covered information has been effective to fulfill the purposes of this title;

(E) whether the kinds of covered information submitted have been appropriate and useful, or overbroad or overnarrow;

(F) whether the protections of covered information allow for adequate accountability and transparency of the regulatory, enforcement, and other aspects of implementing this title; and

(G) any other factors at the discretion of the Inspector General of the Department.

SEC. 107. ANNUAL ASSESSMENT OF CYBERSECURITY.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, and every year thereafter, the Council shall submit to the appropriate congressional committees a report on the effectiveness of this title in reducing the risk of cyber attack to critical infrastructure.

(b) CONTENTS.—Each report submitted under subsection (a) shall include—

(1) a discussion of cyber risks and associated consequences and whether the cybersecurity practices developed under section 103 are sufficient to effectively remediate and mitigate cyber risks and associated consequences; and

(2) an analysis of—

(A) whether owners of critical cyber infrastructure are successfully implementing the cybersecurity practices adopted under section 103;

(B) whether the critical infrastructure of the United States is effectively secured from cybersecurity threats, vulnerabilities, and consequences; and

(C) whether additional legislative authority or other actions are needed to effectively remediate or mitigate cyber risks and associated consequences.

(c) FORM OF REPORT.—A report submitted under this subsection shall be submitted in an unclassified form, but may include a classified annex, if necessary.

SA 2732. Mr. REID (for Mr. FRANKEN) proposed an amendment to amendment SA 2731 proposed by Mr. REID (for Mr. LIEBERMAN (for himself, Ms. COLLINS, Mr. ROCKEFELLER, Mrs. FEINSTEIN, and Mr. CARPER)) to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; as follows:

At the end, add the following new section:

SEC. ____.

Notwithstanding any other provision of this Act, section 701 and section 706(a)(1) shall have no effect.

SA 2733. Mr. REID proposed an amendment to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; as follows:

On page 20, line 5, strike ''180 days'' and insert ''170 days''.

SA 2734. Mr. REID proposed an amendment to amendment SA 2733 proposed by Mr. REID to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; as follows:

In the amendment strike ''170'' and insert ''160''.

SA 2735. Mr. REID proposed an amendment to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; as follows:

At the end, add the following new section:

SEC. ____.

This Act shall become effective 3 days after enactment.

SA 2736. Mr. REID proposed an amendment to amendment SA 2735 proposed by Mr. REID to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; as follows:

In the amendment, strike ''3 days'' and insert ''2 days''.

SA 2737. Mr. REID proposed an amendment to amendment SA 2736 proposed by Mr. REID to the amendment SA 2735 proposed by Mr. REID to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; as follows:

In the amendment, strike ''2 days'' and insert ''1 day''.

SA 2738. Ms. SNOWE (for herself and Mr. WARNER) submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

Beginning on page 23, strike line 19 and all that follows through page 24, line 18, and insert the following:

(1) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to increase, decrease, or otherwise alter the existing authority of any Federal agency to regulate the security of critical cyber infrastructure.

SA 2739. Mrs. GILLIBRAND (for herself and Mr. BENNET) submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

In section 402, strike subsection (a) and insert the following:

(a) ASSESSMENT OF CYBERSECURITY EDUCATION IN COLLEGES, UNIVERSITIES, UNIVERSITY SYSTEMS, NONPROFIT ORGANIZATIONS, AND THE PRIVATE SECTOR.—

(1) REPORT BY THE NATIONAL SCIENCE FOUNDATION.—

(A) REPORT REQUIRED.—Not later than 1 year after the date of enactment of this Act, the Director of the National Science Foundation 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 the state of cybersecurity education in institutions of higher education in the United States.

(B) CONTENTS OF REPORT.—The report required under subparagraph (A) shall include baseline data on—

(i) the state of cybersecurity education in the United States;

(ii) the extent of professional development opportunities for faculty in cybersecurity principles and practices;

(iii) descriptions of the content of cybersecurity courses in undergraduate computer science curriculum;

(iv) the extent of the partnerships and collaborative cybersecurity curriculum development activities that leverage industry and government needs, resources, and tools; and

(v) proposed metrics to assess progress toward improving cybersecurity education.

(2) REPORT BY SECRETARY.—

(A) REPORT REQUIRED.—Not later than 1 year after the date of enactment of this Act, the Secretary 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 the support provided by the Department to education and training programs, including—

(i) the use of resources by the Department;

(ii) how the Secretary plans to use the resources of the Department in the future; and

(iii) the overall strategy of the Department to expand the cybersecurity human capital capacity of the United States.

(B) CONTENTS OF REPORTS.—The report required under subparagraph (A) shall include information on past, planned, or potential support by the Department for education and training programs that—

(i) emphasize experiential learning and the opportunity to take on significant real-world casework as integral parts of training and development programs for cybersecurity professions;

(ii) demonstrate a current and projected caseload of sufficient, important system and network defense activity to provide real-world training opportunities for trainees, with a heavy emphasis on real-life, hands-on, high-level cybersecurity work;

(iii) demonstrate practical computer network defense skills and up-to-date cybersecurity experience of the senior staff proposing to lead the education and training programs;

(iv) demonstrate access to hands-on training programs in the most up-to-date computer network defense technologies and techniques; and

(v) collaborate or plan to collaborate with the Federal Government, including laboratories of the Department of Defense and the Department of Energy, State or local governments, or private sector companies in the United States.

SA 2740. Mr. LIEBERMAN (for Mr. NELSON of Florida) proposed an amendment to the resolution S. Res. 525, honoring the life and legacy of Oswaldo Paya Sardinas; as follows:

On page 4, line 13, strike ''; and'' and insert a semicolon.

On page 4, line 17, strike the period and insert ''; and''.

On page 4, after line 17, insert the following:

(7) condemns the Government of Cuba for the detention of nearly 50 pro-democracy activists following the memorial service for Oswaldo Payá Sardiñas.

SA 2741. Mr. BLUMENTHAL submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 27, strike line 13 and all that follows through page 30, line 19, and insert the following:

(ii) submit to the Council an application for an assessment described in subsection (b)(1)(B) by a qualified third-party private entity verifying that the owner has developed and effectively implemented cybersecurity measures sufficient to satisfy the outcome-based cybersecurity practices established under section 103.

(4) CERTIFICATION.—

(A) SELF-CERTIFICATION.—Upon receipt of a self-certification under paragraph (3)(B)(i), the Council shall certify an owner.

(B) ASSESSMENT APPLICATION.—

(i) IN GENERAL.—Upon receipt of an application by an owner for an assessment under paragraph (3)(B)(ii), the Council shall direct a qualified third-party private entity to conduct an assessment of the owner in accordance with an agreement described in subsection (b)(1).

(ii) IN COMPLIANCE.—If a qualified third-party private entity determines an owner is in compliance with all applicable cybersecurity practices, the Council shall certify the owner.

(5) NONPERFORMANCE.—If the Council determines that a certified owner is not in compliance with the cybersecurity practices established under section 103, the Council shall—

(A) notify the certified owner of such determination; and

(B) work with the certified owner to remediate promptly any deficiencies.

(6) REVOCATION.—If a certified owner fails to remediate promptly any deficiencies identified by the Council, the Council shall revoke the certification of the certified owner.

(7) REDRESS.—

(A) IN GENERAL.—If the Council revokes a certification under paragraph (6), the Council shall—

(i) notify the owner of such revocation; and

(ii) provide the owner with specific cybersecurity measures that, if implemented, would remediate any deficiencies.

(B) RECERTIFICATION.—If the Council determines that an owner has remedied any deficiencies and is in compliance with the cybersecurity practices, the Council may recertify the owner.

(b) ASSESSMENTS.—

(1) THIRD-PARTY ASSESSMENTS.—The Council shall—

(A) develop qualifications for third-party private entities that ensure that the entity has—

(i) substantial expertise in cybersecurity;

(ii) the expertise necessary to perform third-party audits of the cybersecurity of critical cyber infrastructure systems and assets;

(iii) adopted appropriate policies and procedures to ensure that the entity provides independent analysis that is not affected by any conflict of interest or colored by any business interest that the entity may hold; and

(iv) any other qualifications determined relevant by the Council; and

(B) in consultation with owners and operators and the Critical Infrastructure Protection Advisory Council, shall enter into agreements with qualified third-party private entities, to conduct assessments that use reliable, repeatable, performance-based evaluations and metrics to assess whether an owner submitting an application under subsection (a)(3)(B)(ii) is in compliance with all applicable cybersecurity practices.

(2) TRAINING.—The Council shall ensure that third party assessors described in paragraph (1) undergo regular training and accreditation.

(3) OTHER ASSESSMENTS.—Using the procedures developed under this section, the Council may perform cybersecurity assessments of a certified owner based on actual knowledge or a reasonable suspicion that the certified owner is not in compliance with the cybersecurity practices or any other risk-based factors as identified by the Council.

(4) NOTIFICATION.—The Council shall provide copies of any assessments by the Federal Government to the certified owner.

(5) ACCESS TO INFORMATION.—

(A) IN GENERAL.—For the purposes of an assessment conducted under this subsection, a certified owner shall provide the Council, or a third party assessor, any reasonable access necessary to complete an assessment.

(B) PROTECTION OF INFORMATION.—Information provided to the Council, the Council's designee, or any assessor during the course of an assessment under this section shall be protected from disclosure in accordance with section 106.

(c) BENEFITS OF CERTIFICATION.—

(1) LIMITATIONS ON CIVIL LIABILITY.—

(A) DEFINITION.—

(i) IN GENERAL.—In this paragraph, the term ''cyber attack'' means an incident determined by the Attorney General to be an unauthorized intrusion or attack on or through a computer system or asset that causes damage or disruption to the operation or integrity of critical infrastructure that results in—

(I) loss of life, serious physical injury, or the substantial interruption of life-sustaining services;

(II) catastrophic economic damage to the United States, including—

(aa) failure or substantial disruption of a United States financial market;

(bb) incapacitation or sustained disruption of a transportation system; or

(cc) other systemic, long-term damage to the United States economy; or

(III) severe degradation of national security or national security capabilities, including intelligence and defense functions.

(ii) NO JUDICIAL REVIEW.—A determination by the Attorney General under clause (i) shall not be subject to judicial review.

(B) LIMITATION.—In any civil action for damages directly caused by a cyber attack, a certified owner shall not be liable for any punitive damages intended to punish or deter if the certified owner is in compliance with the appropriate cybersecurity practices at the time of the incident related to that cyber risk.

SA 2742. Mr. TESTER submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 186, beginning on line 14, strike ''for the timely destruction of cybersecurity threat indicators that'' and insert ''to destroy cybersecurity threat indicators not later than 1 year after such indicators''.

AUTHORITY FOR COMMITTEES TO MEET

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

Ms. SHAHEEN. Mr. President, I ask unanimous consent that the Committee on Commerce, Science, and Transportation be authorized to meet during the session of the Senate on July 31, 2012, at 2:30 p.m. in room SR–253 of the Russell Senate Office Building.

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

COMMITTEE ON ENERGY AND NATURAL RESOURCES

Ms. SHAHEEN. Mr. President, I ask unanimous consent that the Committee on Energy and Natural Resources be authorized to meet during the session of the Senate on July 31, 2012, at 10 a.m. in room SD–366 of the Dirksen Senate Office Building.

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

COMMITTEE ON FOREIGN RELATIONS

Ms. SHAHEEN. Mr. President, I ask unanimous consent that the Committee on Foreign Relations be authorized to meet during the session of the Senate on July 31, 2012, at 10 a.m.

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

SELECT COMMITTEE ON INTELLIGENCE

Ms. SHAHEEN. Mr. President, I ask unanimous consent that the Select Committee on Intelligence be authorized to meet during the session of the Senate on July 31, 2012, at 2:30 p.m.

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

SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL WORKFORCE, AND THE DISTRICT OF COLUMBIA

Ms. SHAHEEN. Mr. President, I ask unanimous consent that the Committee on Homeland Security and Governmental Affairs' Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia be authorized to meet during the session of the Senate on July 31, 2012, at 10 a.m. to conduct a hearing entitled, ''State of Federal Privacy and Data Security Law: Lagging Behind the Times?''

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

SUBCOMMITTEE ON WESTERN HEMISPHERE, PEACE CORPS, AND GLOBAL NARCOTICS AFFAIRS

Ms. SHAHEEN. Mr. President, I ask unanimous consent that the Committee on Foreign Relations be authorized to meet during the session of the Senate on July 30, 2012, at 2 p.m., to hold a Western Hemisphere, Peace Corps, and Global Narcotics Affairs subcommittee hearing entitled, ''Doing Business in Latin America: Positive Trends but Serious Challenges.''

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

PRIVILEGES OF THE FLOOR

Mr. HARKIN. Mr. President, I ask unanimous consent that Oliver O'Connor and Kevin Burgess of my staff be granted floor privileges for the duration of today's session.

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

FOREIGN TRAVEL FINANCIAL REPORTS

In accordance with the appropriate provisions of law, the Secretary of the Senate herewith submits the following reports for standing committees of the Senate, certain joint committees of the Congress, delegations and groups, and select and special committees of the Senate, relating to expenses incurred in the performance of authorized foreign travel:

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON APPROPRIATIONS FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Paul Grove:									
Bahrain	Dinar		364.24						364.24
Pakistan	Rupee		40.00						40.00
Afghanistan	Afghani		112.00						112.00
Iraq	Dinar		276.00						276.00
United States	Dollar				12,435.60				12,435.60
Adrienne Hallett:									
Côte d'Ivoire	Franc		436.00						436.00
Namibia	Rand		457.00						457.00
South Africa	Rand		994.09						994.09
Morocco	Dirahm		300.48						300.48
Zambia	Dollar		278.43						278.43
Erik Fatemi:									
Côte d'Ivoire	Franc		436.00						436.00
Namibia	Rand		457.00						457.00
South Africa	Rand		994.09						994.09
Morocco	Dirahm		300.48						300.48
Zambia	Dollar		278.43						278.43
Senator Thad Cochran:									
Turkey	Lira		589.03						589.03
Thailand	Baht		974.28						974.28
China	Yuan		736.18						736.18
Korea	Won		683.02						683.02
Stewart Holmes:									
Turkey	Lira		589.03						589.03
Thailand	Baht		608.85						608.85
China	Yuan		736.18						736.18
Korea	Won		683.02						683.02
Kay Webber:									
Turkey	Lira		589.03						589.03

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON APPROPRIATIONS FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012—Continued

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Thailand	Baht		608.85						608.85
China	Yuan		736.18						736.18
Korea	Won		683.02						683.02
Total			13,940.91		12,435.60		0.00		26,376.51

SENATOR DANIEL K. INOUYE,
Chairman, Committee on Appropriations, July 20, 2012.

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON ARMED SERVICES FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Senator Lindsey Graham:									
United States	Dollar				13,175.70				13,175.70
United Arab Emirates	Dollar		27.23						27.23
Senator Mark Begich:									
United States	Dollar				11,592.80				11,592.80
Croatia	Kuna		110.31						110.31
David Ramseur:									
United States	Dollar				15,703.00				15,703.00
Croatia	Kuna		70.11						70.11
Adam J. Barker:									
United States	Dollar				8,089.12				8,089.12
Uganda	Dollar		343.00						343.00
South Sudan	Dollar		300.00						300.00
Michael J. Noblet:									
United States	Dollar				8,545.00				8,545.00
Uganda	Shilling		511.00						511.00
South Sudan	Pound		383.00						383.00
Gordon Peterson:									
United States	Dollar				17,196.10				17,196.10
Japan	Yen		1,134.01						1,134.01
Thailand	Baht		594.07						594.07
Burma	Kyat		312.00						312.00
David N. Bonine:									
United States	Dollar				18,611.90				18,611.90
Japan	Yen		1,113.00						1,113.00
Thailand	Baht		544.00						544.00
Burma	Kyat		340.00						340.00
Senator Jim Webb:									
United States	Dollar				17,192.90				17,192.90
Japan	Yen		1,293.01						1,293.01
Thailand	Baht		810.07						810.07
Burma	Kyat		514.00						514.00
Michael J. Kuiken:									
United States	Dollar				8,679.00				8,679.00
Uganda	Shilling		526.00						526.00
South Sudan	Pound		384.00						384.00
Senator John McCain:									
United States	Dollar				9,979.96				9,979,96
Turkey	Dollar		860.58						860.58
Lithuania	Dollar		230.13						230.13
Jordan	Dollar		68.62						68.62
United States	Dollar				14,388.40				14,388.40
Senator Joseph I. Lieberman:									
United States	Dollar				1,154.40				1,154.40
Turkey	Dollar		782.58						782.58
Senator James M. Inhofe:									
Ghana	Cedi		11.14						11.14
Tanzania	Shilling		119.31						119.31
United Arab Emirates	Dirham		176.19						176.19
Anthony Lazarski:									
Ghana	Cedi		11.14						11.14
Tanzania	Shilling		115.53						115.53
United Arab Emirates	Dirham		82.25						82.25
Mark Powers:									
Ghana	Cedi		11.14						11.14
Tanzania	Shilling		129.89						129.89
United Arab Emirates	Dirham		107.71		78.28				185.99
Luke Holland:									
Ghana	Cedi		11.14						11.14
Tanzania	Shilling		152.46						152.46
United Arab Emirates	Dirham		134.91		78.28				213.19
Germany	Euro		15.40						15.40
Vance Serchuk:									
Saudi Arabia	Dollar		176.00						176.00
Lebanon	Dollar		247.00						247.00
Israel	Dollar		832.00						832.00
William G.P. Monahan:									
United States	Dollar				13,331.00		34.25		13,365.25
Afghanistan	Dollar		35.00						35.00
Turkey	Dollar		215.00						215.00
Belgium	Dollar		248.86						248.86
Senator John McCain:									
United States	Dollar				13,030.20				13,030.20
Malaysia	Dollar		186.98						186.98
Singapore	Dollar		190.02						190.02
Senator Joseph I. Lieberman:									
United States	Dollar				9,962.80				9,962.80
Saudi Arabia	Dollar		863.01						863.01
Israel	Dollar		2,054.88						2,054.88
Margaret Goodlander:									
United States	Dollar				10,129.80				10,129.80
Saudi Arabia	Dollar		912.14						912.14
Lebanon	Dollar		141.00						141.00
Israel	Dollar		1,947.94						1,947.94
United States	Dollar				21,584.10				21,584.10

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON ARMED SERVICES FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012—Continued

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Malaysia	Dollar		421.62						421.62
Singapore	Dollar		527.41						527.41
Senator Joseph I. Lieberman:									
United States	Dollar				20,232.30				20,232.30
Malaysia	Dollar		444.00						444.00
Singapore	Dollar		1,192.00						1,192.00
Christian D. Brose:									
United States	Dollar				17,292.90				17,292.90
Malaysia	Dollar		166.00						166.00
Singapore	Dollar		97.00						97.00
United States	Dollar				14,772.70				14,772.70
Lithuania	Dollar		96.00						96.00
Jordan	Dollar		228.00						228.00
Richard D. DeBobes:									
United States	Dollar				10,128.00		29.00		10,157.00
Afghanistan	Dollar		35.00						35.00
Turkey	Dollar		215.00						215.00
Belgium	Euro		248.86						248.86
Senator Jack Reed:									
United States	Dollar				10,302.90				10,302.90
Afghanistan	Dollar		20.00						20.00
Turkey	Dollar		52.00						52.00
Belgium	Dollar		16.00						16.00
Carolyn Chuhta:									
United States	Dollar				13,331.90				13,331.90
Afghanistan	Dollar		20.00						20.00
Turkey	Dollar		52.00						52.00
Belgium	Dollar		16.00						16.00
Vance Serchuk:									
United States	Dollar				20,232.30				20,232.30
Malaysia	Dollar		506.00						506.00
Singapore	Dollar		617.00						617.00
Christian D. Brose:									
United States	Dollar				6,480.06				6,480.06
Turkey	Dollar		563.00						563.00
Senator James M. Inhofe:									
Montenegro	Euro		52.32						52.32
Italy	Euro		138.65						138.65
Anthony Lazarski:									
Montenegro	Euro		52.32						52.32
Italy	Euro		136.72		43.09				179.81
Mark Powers:									
Montenegro	Euro		52.32						52.32
Italy	Euro		70.22		25.35				95.57
Joseph M. Bryan:									
United States	Dollar				16,874.20				16,874.20
Republic of Korea	Won		542.91						542.91
Japan	Yen		906.93		55.00				961.93
Ozge Cuzelsu:									
United States	Dollar				15,104.10				15,104.10
Republic of Korea	Won		560.00		20.00				580.00
Japan	Yen		1,029.18		95.00				1,124.18
Senator Ben Nelson:									
United States	Dollar				13,461.20				13,461.20
Egypt	Pound		450.00						450.00
Saudi Arabia	Riyal		548.00						548.00
Ryan Ehly:									
United States	Dollar				13,461.20				13,461.20
Egypt	Pound		447.00						447.00
Saudi Arabia	Riyal		538.00						538.00
Senator Rob Portman:									
United States	Dollar				12,471.00				12,471.00
Israel	Dollar		1,083.38						1,083.38
Jordan	Dollar		217.55				37.13		254.68
United Arab Emirates	Dollar		286.16						286.16
Afghanistan	Dollar		13.00						13.00
Brent Bombach:									
United States	Dollar				12,825.20				12,825.20
Israel	Dollar		538.40						538.40
Jordan	Dollar		217.53						217.53
United Arab Emirates	Dollar		286.16						286.16
Afghanistan	Dollar		13.00						13.00
Senator Carl Levin:									
United States	Dollar				12,346.00				12,346.00
Afghanistan	Dollar		35.00						35.00
Turkey	Dollar		214.97						214.97
Belgium	Dollar		248.86				45.32		294.18
Total			34,590.23		422,057.14		145.70		456,793.07

SENATOR CARL LEVIN,
Chairman, Committee on Armed Services, July 18, 2012.

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Senator Roger Wicker:									
Ivory Coast	Franc		436.00						436.00
Namibia	Rand		278.43						278.43
South Africa	Rand		994.09						994.09
Zambia	Kwacha		278.43						278.43
Morocco	Dirham		300.48						300.48
Senator Richard Shelby:									
Italy	Euro		408.00						408.00
Hungary	Forint		450.00						450.00
Austria	Euro		645.00						645.00
Switzerland	Franc		458.00						458.00

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012—Continued

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Spain	Euro		579.00						579.00
Slovakia	Euro		286.00						286.00
Jonathan Graffeo:									
Italy	Euro		408.00						408.00
Hungary	Forint		450.00						450.00
Austria	Euro		645.00						645.00
Switzerland	Franc		458.00						458.00
Spain	Euro		579.00						579.00
Slovakia	Euro		286.00						286.00
William Duhnke:									
Italy	Euro		408.00						408.00
Hungary	Forint		450.00						450.00
Austria	Euro		645.00						645.00
Switzerland	Franc		458.00						458.00
Spain	Euro		579.00						579.00
Slovakia	Euro		286.00						286.00
Total			10,765.43						10,765.43

SENATOR TIM JOHNSON,
Chairman, Committee on Banking, Housing, and Urban Affairs, July 23, 2012.

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON THE BUDGET FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Senator Kent Conrad:									
Cote d'Ivoire	CFA Franc		436.00						436.00
Botswana	Pula		578.00						578.00
Malawi	Kwacha		279.00						279.00
Zambia	Kwacha		556.86						556.86
Morocco	Dirham		300.48						300.48
Total			2,150.34						2,150.34

SENATOR KENT CONRAD,
Chairman, Senate Budget Committee, July 11, 2012.

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON ENERGY AND NATURAL RESOURCES FOR TRAVEL FROM APR. 1 TO JUNE 30, 2102

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Senator Jeff Bingaman:									
United States	Dollar				15,238.80				15,238.80
Hong Kong	HKD		1,220.17						1,220.17
China	Yuan		1,283.92						1,283.92
Jonathan Black:									
United States	Dollar				12,443.50				12,443.50
Hong Kong	HKD		1,358.48						1,358.48
China	Yuan		1,422.23						1,422.23
Michael Carr:									
United States	Dollar				8,216.60				8,216.60
Hong Kong	HKD		1,520.98						1,520.98
China	Yuan		1,409.73						1,409.73
Robert Simon:									
United States	Dollar				11,795.30				11,795.30
Hong Kong	HKD		1,210.16						1,210.16
China	Yuan		1,244.62						1,244.62
Delegation expenses:									
Hong Kong	HKD						1,854.71		1,854.71
China	Yuan						2,527.69		2,527.69
Total			10,670.29		47,694.20		4,382.40		62,746.89

SENATOR JEFF BINGAMAN,
Chairman, Committee on Energy and Natural Resources, July 18, 2012.

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON THE ENVIRONMENT AND PUBLIC WORKS FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Senator John Boozman:									
Ghana	Cedi		11.14						11.14
Tanzania	Shilling		118.57						118.57
United Arab Emirates	Dirhams		200.84						200.84
Germany	Euros		56.47						56.47
Senator Barbara Boxer:									
United States	Dollar				5,815.95				5,815.95
Brazil	Real		437.22						437.22
Argentina	Peso		1,468.09						1,468.09
United States	Dollar				10,932.80				10,932.80
France	Euro		3,856.00						3,856.00

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON THE ENVIRONMENT AND PUBLIC WORKS FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012—Continued

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Bettina Poirier:									
United States	Dollar				9,393.55				9,393.55
Brazil	Real		148.00						148.00
Argentina	Peso		1,468.09						1,468.09
Mary Kerr:									
United States	Dollar				9,393.55				9,393.55
Brazil	Real		148.00						148.00
Argentina	Peso		1,468.09						1,468.09
United States	Dollar				10,932.80				10,932.80
France	Euro		3,856.00						3,856.00
Paul Ordal:									
United States	Dollar				9,393.55		110.00		9,503.55
Brazil	Real		148.00						148.00
Argentina	Peso		1,468.09						1,468.09
United States	Dollar				10,932.80		361.00		11,293.80
France	Euro		3,856.00						3,856.00
Total			18,708.60		66,795.00		471.00		85,974.60

SENATOR BARBARA BOXER,
Chairman, Committee on the Environment and Public Works,
July 19, 2012.

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON FINANCE FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Amber Cottle:									
Russia	Ruble		1,428.12						1,428.12
United States	Dollar				8,969.92				8,969.92
Bruce Hirsh:									
Russia	Ruble		1,236.37						1,236.37
United States	Dollar				8,969.92				8,969.92
Chelsea Thomas:									
Russia	Ruble		1,380.85						1,380.85
United States	Dollar				8,969.92				8,969.92
Hun Quach:									
Russia	Ruble		1,339.74						1,339.74
United States	Dollar				8,969.92				8,969.92
Catharine Bailey:									
Russia	Ruble		1,012.20						1,012.20
United States	Dollar				4,822.92				4,822.92
Lauren Bazel:									
Russia	Ruble		1,048.40						4,048.40
United States	Dollar				8,969.92				8,969.92
Ryan McComick:									
Russia	Ruble		1,145.20						1,145.20
United States	Dollar				4,822.92				4,822.92
Karin Hope:									
Russia	Ruble		1,166.65						1,166.65
United States	Dollar				8,969.92				8,969.92
Paul Poteet:									
Russia	Ruble		1,203.80						1,203.80
United States	Dollar				8,969.92				8,969.92
Jeffry Phan:									
Russia	Ruble		1,034.55						1,034.55
United States	Dollar				8,969.92				8,969.92
Ann Hawks:									
Russia	Ruble		1,024.64						1,024.64
United States	Dollar				4,822.92				4,822.92
Jayme White:									
Russia	Ruble		1,275.10						1,275.10
United States	Dollar				8,969.92				8,969.92
Everett Eissenstat:									
Russia	Ruble		1,208.60						1,208.60
United States	Dollar				8,969.92				8,969.92
Gregory Kalbaugh:									
Russia	Ruble		1,050.71						1,050.71
United States	Dollar				8,969.92				8,969.92
Amanda Slater:									
Russia	Ruble		1,099.38						1,099.38
United States	Dollar				8,969.92				8,969.92
Jonathan Cordone:									
Russia	Ruble		1,424.49						1,424.49
United States	Dollar				4,822.92				4,822.92
Thomas Mahr:									
Russia	Ruble		1,114.39						1,114.39
United States	Dollar				4,822.92				4,822.92
Keith Franks:									
Russia	Ruble		1,145.42						1,145.42
United States	Dollar				8,969.92				8,969.92
Delegation Expenses:*									
Russia	Dollar						8,567.73		8,567.73
Gabriel Adler:									
Myanmar	Kyat		1,022.73						1,022.73
United States	Dollar				13,226.00				13,226.00
Everett Eissenstat:									
Myanmar	Kyat		974.99						974.99
United States	Dollar				13,226.00				13,226.00
Delegation Expenses:*									
Myanmar	Dollar				2,948.09		3,578.25		6,526.34
Total			23,336.33		170.123.65		12,145.98		205,605.96

SENATOR MAX BAUCUS,
Chairman, Committee on Finance, July 20, 2012.

*Delegation expenses include interpretation, transportation, embassy overtime, as well as other official expenses in accordance with the responsibilities of the host country.

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON FOREIGN RELATIONS FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Senator John Barrasso:									
Turkey	Lira		615.85						615.85
Thailand	Baht		889.78						889.78
China	Renminbi		668.73						668.73
Korea	Won		469.62						469.62
Senator Christopher Coons:									
Uganda	Shilling		862.68						862.68
Kenya	Shilling		1,015.00						1,015.00
Tanzania	Shilling		309.84						309.84
Egypt	Pound		195.00						195.00
United States	Dollar				11,148.60				11,148.60
Senator Richard Durbin:									
Ukraine	Hryvna		237.93						237.93
Turkey	Lira		506.88						506.88
Georgia	Lari		455.67						455.67
Armenia	Dram		157.77						157.77
United States	Dollar				13,525.80				13,525.80
Senator John Kerry:									
Afghanistan	Dollar		19.00						19.00
United Arab Emirates	Dirham		1,082.60						1,082.60
Israel	Shekel		340.00						340.00
Egypt	Pound		781.66						781.66
Jordan	Dinar		54.00						54.00
France	Euro		498.91						498.91
United States	Dollar				12,834.60				12,834.60
Senator Marco Rubio:									
Colombia	Peso		1,242.29						1,242.29
United States	Dollar				1,826.90				1,826.90
Senator Tom Udall:									
Côte D'Ivoire	Franc		436.00						436.00
Namibia	Rand		556.00						556.00
South Africa	Rand		994.09						994.09
Zambia	Dollar		278.43						278.43
Morocco	Dirham		300.48						300.48
Perry Cammack: :									
United Arab Emirates	Dirham		608.56						608.56
Israel	Shekel		404.70						404.70
Egypt	Pound		877.52						877.52
United States	Dollar				2,253.90				2,253.90
Victor Cervino:									
Colombia	Peso		952.29						952.29
United States	Dollar				1,826.90				1,826.90
William Danvers:									
Afghanistan	Dollar		19.00						19.00
United Arab Emirates	Dirham		748.99						748.99
Israel	Shekel		340.00						340.00
Egypt	Pound		544.40						544.40
Jordan	Dinar		94.59						94.59
France	Euro		508.91						508.91
United States	Dollar				15,237.60				15,237.60
Chris Homan:									
Ukraine	Hryvna		237.93						237.93
Turkey	Lira		446.94						446.94
Georgia	Lari		455.67						455.67
Armenia	Dram		175.38						175.38
United States	Dollar				9,267.60				9,267.60
Alex Lee:									
Mexico	Peso		1,381.66						1,381.66
United States	Dollar				1,073.59				1,073.59
Emily Mendrala:									
Mexico	Peso		1,373.66						1,373.66
United States	Dollar				1,073.59				1,073.59
Melanie Nakagawa:									
Brazil	Real		3,998.41						3,998.41
United States	Dollar				1,601.90				1,601,90
Ann Norris:									
France	Euro		3,561.00						3,561.00
United States	Dollar				1,208.60				1,208.60
Matthew Padilla:									
Mexico	Peso		1,087.66						1,087.66
United States	Dollar				1,130.40				1,130.40
Michael Phelan:									
India	Rupee		2,503.00						2,503.00
United States	Dollar				11,075.95				11,075.95
Rolfe Michael Schiffer:									
Japan	Yen		425.00						425.00
Burma	Kyat		395.00						395.00
Singapore	Dollar		657.00						657.00
Korea	Won		184.00						184.00
United States	Dollar				16,853.90				16,853.90
Halie Soifer:									
Uganda	Shilling		903.68						903.68
Kenya	Shilling		904.00						904.00
Tanzania	Shilling		358.84						358.84
Egypt	Pound		185.05						185.05
United States	Dollar				11,018.60				11,018.60
Joel Starr:									
Ghana	Cedi		241.00						241.00
Tanzania	Shilling		630.00						630.00
United Arab Emirates	Dirham		406.61						406.61
Germany	Euro		175.06						175.06
Fatema Sumar:									
United Arab Emirates	Dirham		198.00						198.00
Afghanistan	Dollar		83.00						83.00
United States	Dollar				12,512.70				12,512.70
Megan Thompson:									
Guatemala	Quetzal		812.63						812.63
United States	Dollar				798.00				798.00
Atman Trivedi:									
Singapore	Dollar		166.00						166.00
Indonesia	Rupiah		254.00		1,023.40				1,277.40
Malaysia	Ringgit		339.00						339.00
United States	Dollar				12,172.20				12,172.20
Victoria Woodbury:									
Spain	Euro		2,072.00		645.40				2,717.40

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON FOREIGN RELATIONS FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012—Continued

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
United States	Dollar				1,462.20				1,462.20
Total			42,698.35		141,572.33				184,250.68

SENATOR JOHN F. KERRY,
Chairman, Committee on Foreign Relations, July 20, 2012.

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Senator Susan M. Collins:									
United States	Dollar				11,777.80				11,777.80
Thailand	Baht		836.54						836.54
Burma	Kyat		88.00						88.00
Rob Epplin:									
United States	Dollar				13,424.80				13,424.80
Thailand	Baht		836.54						836.54
Burma	Kyat		88.00						88.00
Vance Serchuk:									
United States	Dollar				5,831.00				5,831.00
Turkey	Lira		2,899.00						2,899.00
Israel	Shekel		382.00						382.00
Margaret Goodlander:									
United States	Dollar				6,129.10				6,129.10
Turkey	Lisa		2,899.00						2,899.00
Israel	Shekel		393.00						393.00
Delegation Expenses:									
Thailand	Baht						663.75		663.75
Total			8,422,08		37,162.70		663.75		46,248.53

SENATOR JOSEPH I. LIEBERMAN,
Chairman, Committee on Homeland Security and Governmental Affairs, July 25, 2012.

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON THE JUDICIARY FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Todd Webster:									
United States	Dollar				11,018.60				11,018.60
Uganda	Shilling		918.18						918.18
Kenya	Shilling		928.50						928.50
Tanzania	Shilling		264.34						264.34
Egypt	Pound		253.55						253.55
Total			2,364.57		11,018.60				13,383.17

SENATOR PATRICK J. LEAHY,
Chairman, Committee on the Judiciary, July 20, 2012.

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON HEALTH, EDUCATION, LABOR AND PENSIONS FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Senator Tom Harkin:									
Côte d'Ivoire	Franc		436.00						436.00
Namibia	Rand		556.00						556.00
South Africa	Rand		994.09						994.09
Zambia	Dollar		278.43						278.43
Morocco	Dirahm		300.48						300.48
Senator Michael B. Enzi:									
Côte d'Ivoire	Franc		436.00						436.00
Botswana	Pula		578.00						578.00
Malawi	Kwacha		279.00						279.00
Zambia	Kwacha		556.86						556.86
Morocco	Dirahm		300.48						300.48
Melissa Pfaff:									
Côte d'Ivoire	Franc		436.00						436.00
Botswana	Pula		578.00						578.00
Malawi	Kwacha		476.00						476.00
Zambia	Kwacha		556.86						556.86
Morocco	Dirahm		300.48						300.48
Maria Rosario Gutierrez:									
Côte d'Ivoire	Franc		120.00						120.00
United States	Dollar				4,280.60				4,280.60
Delegation Expenses:*									
Côte d'Ivoire	Franc						15,818.00		15,818.00
Namibia	Rand						15,557.00		15,557.00
South Africa	Rand						14,730.91		14,730.91
Botswana	Pula						3,102.00		3,102.00
Malawi	Kwacha						9,344.65		9,344.65

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON HEALTH, EDUCATION, LABOR AND PENSIONS FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012—Continued

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Zambia	Kwacha						3,227.88		3,227.88
Morocco	Dirahm						13,043.24		13,043.24
Total			7,182.68		4,280.60		74,823.68		86,286.96

SENATOR TOM HARKIN,
Chairman, Committee on Health, Education, Labor, and Pensions,
July 17, 2012.

*Delegation expenses include payments and reimbursements to the Department of State under the authority of Sec. 502(b) of the Mutual Security Act of 1954, as amended by Sec. 22 of P.L. 95–384, and S. Res. 179 agreed to May 25, 1977.

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON SMALL BUSINESS AND ENTREPRENEURSHIP FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Senator Mary L. Landrieu:									
United States	Dollar				3,021.00				3,021.00
Guatemala	Quetzal		881.00						881.00
Alston Walker:									
United States	Dollar				798.00				798.00
Guatemala	Quetzal		881.00						881.00
Amberly McDowell:									
United States	Dollar				798.00				798.00
Guatemala	Quetzal		881.00						881.00
Elizabeth Whitbeck:									
United States	Dollar				798.00				798.00
Guatemala	Quetzal		881.00						881.00
Delegation expenses:									
Guatemala	Quetzal						2,781.60		2,781.60
Total			3,524.00		5,415.00		2,781.60		11,720.60

SENATOR MARY LANDRIEU,
Chairman, Committee on Small Business and
Entrepreneurship, July 20, 2012.

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMITTEE ON INTELLIGENCE FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Christian Cook	Dollar		2,967.08						2,967.08
Brian Monahan	Dollar		3,332.51						3,332.51
Senator Ron Wyden	Dollar		1,803.00						1,803.00
					14,195.90				14,195.90
John Dickas	Dollar		1,299.53						1,299.53
					16,282.08				16,282.08
Neal Higgins	Dollar		907.00						907.00
					10,326.00				10,326.00
Brian Miller	Dollar		1,179.00						1,179.00
					10,326.00				10,326.00
Tressa Guenov	Dollar		857.00						857.00
					10,326.00				10,326.00
Senator Mark Udall	Dollar		2,662.00						2,662.00
Senator Richard Burr	Dollar		3,083.22						3,083.22
Senator Mark Warner	Dollar		2,613.55						2,613.55
Senator Barbara Mikulski	Dollar		1,786.00						1,786.00
					4,524.90				4,524.90
Jennifer Barrett	Dollar		2,645.00						2,645.00
Christian Cook	Dollar		3,223.34						3,223.34
Michael Pevzner	Dollar		3,153.22						3,153.22
Tressa Guenov	Dollar		1,440.00						1,440.00
					4,524.90				4,524.90
Andrew Kerr	Dollar		328.00						328.00
					9,866.20				9,866.20
Ryan Tully	Dollar		328.00						328.00
					9,866.20				9,866.20
Senator Dianne Feinstein	Dollar		542.00						542.00
					12,477.68				12,477.68
Senator Saxby Chambliss	Dollar		1,083.56						1,083.56
					7,216.70				7,216.70
David Grannis	Dollar		508.00						508.00
					12,477.68				12,477.68
Martha Scott Poindexter	Dollar		1,083.56						1,083.56
					6,533.00				6,533.00
Senator Saxby Chambliss	Dollar		3,332.51						3,332.51
Senator Richard Burr	Dollar		3,332.51						3,332.51
Martha Scott Poindexter	Dollar		3,332.51						3,332.51
Tyler Stephens	Dollar		2,967.08						2,967.08
Teresa Ervin	Dollar		2,967.08						2,967.08
Total			52,756.26		128,943.24				181,699.50

SENATOR DIANNE FEINSTEIN,
Chairman, Committee on Intelligence, July 11, 2012.

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), COMMISSION ON SECURITY AND COOPERATION IN EUROPE FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Hon. Alcee Hastings:									
Belgium	Euro		308.00						308.00
Fred Turner:									
Belgium	Euro		350.00						350.00
Austria	Euro		523.10						523.10
United States	Dollar				2,556.70				2,556.70
Ireland	Euro		933.07						933.07
United States	Dollar				1,012.70				1,012.70
Total			2,114.17		3,569.40				5,683.57

BENJAMIN L. CARDIN,
Chairman, Commission on Security and Cooperation in Europe,
July 19, 2012.

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), MAJORITY LEADER FOR TRAVEL FROM APR. 1 TO JUN. 30, 2012

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Ayesha Khanna:									
Russia	Ruble		1,225.25						1,225.25
United States	Dollar				8,804.92				8,804.92
Thomas Ross:									
United States	Dollar				14,754.12				14,754.12
Ethiopia	Birr		527.00						527.00
Uganda	Shilling		600.12						600.12
South Sudan	Pound		377.00						377.00
Total			2,729.37		23,559.04				26,288.41

SENATOR HARRY REID,
Majority Leader, June 20, 2012.

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), REPUBLICAN LEADER FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Thomas Hawkins:									
Turkey	Lira		639.02						639.02
Thailand	Baht		912.58						912.58
China	Renminbi		836.18						836.18
South Korea	Won		783.02						783.02
Jonathan Lieber:									
United States	Dollar				8,934.32				8,934.32
Russia	Ruble		1,105.87						1,105.87
Total			4,276.67		8,934.32				13,210.99

SENATOR MITCH MCCONNELL,
Republican Leader, June 29, 2012.

CONSOLIDATED REPORT OF EXPENDITURE OF FUNDS FOR FOREIGN TRAVEL BY MEMBERS AND EMPLOYEES OF THE U.S. SENATE, UNDER AUTHORITY OF SEC. 22, P.L. 95–384—22 U.S.C. 1754(b), SPECIAL COMMITTEE ON AGING FOR TRAVEL FROM APR. 1 TO JUNE 30, 2012

Name and country	Name of currency	Per diem		Transportation		Miscellaneous		Total	
		Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency	Foreign currency	U.S. dollar equivalent or U.S. currency
Michael Bassett:									
Czech Republic	Crown		450.00						450.00
United States	Dollar				8,461.40				8,461.40
Cara Goldstein:									
Czech Republic	Crown		346.88						346.88
United States	Dollar				8,461.40				8,461.40
Francine Hennie:									
Czech Republic	Crown		455.00						455.00
United States	Dollar				8,461.40				8,461.40
Sarah Levin:									
Czech Republic	Crown		332.28		36.45				368.73
United States	Dollar				8,451.30				8,451.30
Chad Metzler:									
Czech Republic	Crown		272.00		70.00				342.00
United States	Dollar				8,461.70				8,461.70
Joy McGlaun:									
Czech Republic	Crown		547.00						547.00
United States	Dollar				8,461.40				8,461.40
Anne Montgomery:									
Czech Republic	Crown		571.00		17.50				588.50
United States	Dollar				9,587.80				9,587.80
Total			2,974.16		60,470.35				63,444.51

SENATOR HERB KOHL,
Special Committee on Aging, July 25, 2012.

HONORING THE LIFE AND LEGACY OF OSWALDO PAYA SARDINAS

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the Committee on Foreign Relations be discharged from further consideration of S. Res. 525 and that the Senate proceed to its immediate consideration.

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

The clerk will report the resolution by title.

The assistant legislative clerk read as follows:

A resolution (S. Res. 525) honoring the life and legacy of Oswaldo Paya Sardinas.

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

Mr. NELSON of Florida. Mr. President, I wish to speak about Oswaldo Paya, a Cuban dissident, and his untimely death in Cuba in a supposed automobile accident. The Cuban people, indeed all freedom-loving people of the world, have recently lost a great advocate for freedom. He was someone who was in peaceful opposition to the tyranny that is on the island of Cuba.

Oswaldo Paya died in a car crash on Sunday, July 22. He was just 60 years old. Another Cuban dissident, Harold Cepero, was also killed in the accident, and two European politicians, one from Spain and one from Sweden, were injured. Paya was one of Cuba's best known dissidents. He pushed for civil and human rights. He pushed for an end to one-party rule. He pushed for freedom for political prisoners. And he pushed for support for private businesses. In 2002, his Varela Project delivered more than 24,000 verifiable signatures in support of these ideals to the Cuban Government. It was the largest petition drive in Cuban history. Paya bravely led this initiative at great risk to himself, to his loved ones, and to his colleagues. For his work, he received the European Parliaments' Sakarov Prize for Freedom of Thought in 2002, and he was nominated for the Nobel Peace Prize.

The reason I am bringing this up, other than pointing out that planet Earth has lost a friend for freedom, is to note that the circumstances of the car accident are the topic of some debate. Cuban officials insist the driver was speeding and that he lost control and he hit a tree. But others are saying that witnesses saw another vehicle hit Mr. Paya's vehicle and drive it off the road. Paya's daughter Rosa Maria says she holds the Cuban Government responsible. She has told CNN en Espanol that ''we think it's not an accident. They wanted to do harm and then ended up killing my father.'' That is a direct quote.

Paya's loved ones and the Cuban people and the international community deserve to have all the facts surrounding this tragic event examined and put out in the public. That is why I have submitted, along with a number of our colleagues, S. Res. 525, which honors the life, legacy, and exemplary leadership of Oswaldo Paya. This resolution also calls on the Cuban Government to allow an impartial third-party investigation into the accident. I urge the Senate to unanimously pass this resolution.

This request comes on the heels of other disturbing news out of Cuba. We have learned that more than 40 pro-democracy activists were detained after Paya's funeral last Tuesday. The reason? They dared to shout ''libertad'' at that time—''freedom''—during the ceremony. Reports also indicate that several of the dissidents were severely beaten.

These peaceful activists were only honoring one of their own and they ended up as victims of an authoritarian regime. Now more than ever before the United States must continue policies that promote the fundamental principles of political freedom, democracy, and human rights, to all of which Oswaldo Paya devoted his life.

Senator DURBIN, we are quite concerned the Castro regime continues to hold an American hostage, Alan Gross. Once again, another Senator rises to urge the Cuban regime in the strongest possible terms to immediately and unconditionally release him.

We will never forget Paya's passion and dedication to freedom and faith. The least the regime can do is to release Alan Gross.

Mr. LIEBERMAN. Mr. President, I further ask that the amendment offered by the Senator from Florida, Mr. NELSON, which is at the desk, be agreed to; the resolution, as amended, be agreed to; the preamble be agreed to; the motions to reconsider be made and laid upon the table, with no interviewing action or debate, and that any statements relating to the measure be printed in the RECORD at the appropriate place as if read.

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

The amendment (No. 2740) was agreed to, as follows:

(Purpose: To condemn the Government of Cuba for the detention of nearly 50 pro-democracy activists following the memorial service for Oswaldo Payá Sardiñas)

On page 4, line 13, strike ''; and'' and insert a semicolon.

On page 4, line 17, strike the period and insert ''; and''.

On page 4, after line 17, insert the following:

(7) condemns the Government of Cuba for the detention of nearly 50 pro-democracy activists following the memorial service for Oswaldo Payá Sardiñas.

The resolution (S. Res. 525), as amended, was agreed to.

The preamble was agreed to.

The resolution, as amended, with its preamble, reads as follows:

S. RES. 525

Whereas, on Sunday, July 22, 2012, 60-year-old Cuban dissident and activist Oswaldo Payá Sardiñas died in a car crash in Bayamo, Cuba;

Whereas at a young age, Oswaldo Payá Sardiñas criticized the communist government in Cuba, which led to his imprisonment at a work camp on Cuba's Isle of Youth in 1969;

Whereas, in 1988, Oswaldo Payá Sardiñas founded the Christian Liberation Movement as a nondenominational political organization to further civil and human rights in Cuba;

Whereas, in 1992, Oswaldo Payá Sardiñas announced his intention to run as a candidate to be a representative on the National Assembly of Popular Power of Cuba and, 2 days before the election, was detained by police at his home and determined by Communist Party officials to be ineligible to run for office because he was not a member of the Communist Party;

Whereas, in 1997, Oswaldo Payá Sardiñas collected hundreds of signatures to support his candidacy to the National Assembly of Popular Power, which was rejected by the electoral commission of Cuba;

Whereas the Constitution of Cuba supposedly guarantees the right to a national referendum on any proposal that achieves 10,000 or more signatures from citizens of Cuba who are eligible to vote;

Whereas, in 1998, Oswaldo Payá Sardiñas and other leaders of the Christian Liberation Movement created the Varela Project, a signature drive to secure a national referendum on ''convert[ing] into law, the right of freedom of speech, the freedom of press and freedom of enterprise'';

Whereas, in May 2002, the Varela Project delivered 11,020 signatures from eligible citizens of Cuba to the National Assembly of Popular Power, calling for an end to 4 decades of one-party rule, to which the Government of Cuba responded by beginning its own referendum that made Cuba's socialist system ''irrevocable'', even after an additional 14,000 signatures were added to the Varela Project petition;

Whereas the Varela Project is the largest civil society-led petition in the history of Cuba;

Whereas Oswaldo Payá Sardiñas bravely led the Varela Project at great risk to himself, his loved ones, and his associates;

Whereas, in March 2003, the Government of Cuba arrested 75 human rights activists, including 25 members of the Varela Project, in the crackdown known as Cuba's ''Black Spring'';

Whereas Oswaldo Payá Sardiñas's dedication to freedom and faith earned him the Sakarov Prize for Freedom of Thought from the European Parliament in 2002;

Whereas Oswaldo Payá Sardiñas received the W. Averell Harriman Democracy Award from the United States National Democratic Institute for International Affairs in 2003;

Whereas Oswaldo Payá Sardiñas was nominated for the Nobel Peace Prize by Václav Havel, the former president of the Czech Republic, in 2005; and

Whereas President Barack Obama stated, ''We continue to be inspired by Payá's vision and dedication to a better future for Cuba, and believe that his example and moral leadership will endure.'': Now, therefore, be it

Resolved, That the Senate—

(1) recognizes and honors the life and exemplary leadership of Oswaldo Payá Sardiñas;

(2) offers heartfelt condolences to the family, friends, and loved ones of Oswaldo Payá Sardiñas;

(3) praises the bravery of Oswaldo Payá Sardiñas and his colleagues for collecting more than 11,000 verified signatures in support of the Varela Project;

(4) in memory of Oswaldo Payá Sardiñas, calls on the United States to continue policies that promote respect for the fundamental principles of religious freedom, democracy, and human rights in Cuba, in a

manner consistent with the aspirations of the people of Cuba;

(5) in memory of Oswaldo Payá Sardiñas, calls on the Government of Cuba to provide its citizens with internationally accepted standards for civil and human rights and the opportunity to vote in free and fair elections;

(6) calls on the Government of Cuba to allow an impartial, third-party investigation into the circumstances surrounding the death of Oswaldo Payá Sardiñas; and

(7) condemns the Government of Cuba for the detention of nearly 50 pro-democracy activists following the memorial service for Oswaldo Payá Sardiñas.

ORDERS FOR WEDNESDAY, AUGUST 1, 2012

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that when the Senate completes its business today, it adjourn until 9:30 a.m., on Wednesday, August 1; that following the prayer and pledge, the Journal of proceedings be approved to date, the morning hour be deemed expired, and the time for the two leaders be reserved for their use later in the day; that the majority leader be recognized, and the first hour be equally divided and controlled between the two leaders or their designees, with the Republicans controlling the first half and the majority controlling the final half.

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

PROGRAM

Mr. LIEBERMAN. Mr. President, the majority leader filed cloture on the cyber security bill today. As a result, the filing deadline for first-degree amendments to S. 3414 is 1 p.m. on Wednesday.

I want to indicate to my colleagues that we continue to work on an agreement on amendments to the bill which I hope we can reach. If no agreement is reached, the cloture vote will be on Thursday.

ADJOURNMENT UNTIL 9:30 A.M. TOMORROW

Mr. LIEBERMAN. If there is no further business to come before the Senate, I ask unanimous consent that it adjourn under the previous order.

There being no objection, the Senate, at 7:14 p.m., adjourned until Wednesday, August 1, 2012, at 9:30 a.m.

NOMINATIONS

Executive nominations received by the Senate:

INSTITUTE OF MUSEUM AND LIBRARY SERVICES

ERIC J. JOLLY, OF MINNESOTA, TO BE A MEMBER OF THE NATIONAL MUSEUM AND LIBRARY SERVICES BOARD FOR A TERM EXPIRING DECEMBER 6, 2016, VICE KAREN BROSIUS, TERM EXPIRED.

SUSANA TORRUELLA LEVAL, OF NEW YORK, TO BE A MEMBER OF THE NATIONAL MUSEUM AND LIBRARY SERVICES BOARD FOR A TERM EXPIRING DECEMBER 6, 2015, VICE KATHERINE M. B. BERGER, TERM EXPIRED.