| | | |
|---|---|---|
| McCaskill | Portman | Shelby |
| McConnell | Reed | Sullivan |
| Mikulski | Risch | Thune |
| Moran | Roberts | Tillis |
| Murkowski | Rounds | Toomey |
| Murphy | Sasse | Warner |
| Nelson | Scott | Whitehouse |
| Perdue | Sessions | Wicker |

NOT VOTING—5

| | | |
|---|---|---|
| Cruz | Paul | Vitter |
| Graham | Rubio | |

The amendment (No. 2612), as further modified, was rejected.

The PRESIDING OFFICER. The Senator from Missouri.

Mr. BLUNT. Madam President, I ask unanimous consent to address the floor for up to 15 minutes.

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

Mr. BLUNT. Madam President, last week I came to the floor to express my support for the Cybersecurity Information Sharing Act, which we are dealing with today. The bipartisan vote of 83 to 14 that happened later that day was an important step in the right direction to deal with this issue. The debate has been encouraging. We need to deal with this threat to our economy. It is a threat to our security, it is a threat to our privacy, and we need to deal with it now.

As I and others have said before, if we wait until there is an event that gets people's attention in such a dramatic way that everybody suddenly realizes what is at stake, there is no telling what kind of overreaction Congress will make. This has been a good debate at the time we should have it. Now, of course, we need to move on.

There have been a lot of amendments offered. Many amendments have been accepted by the managers of the bill. With almost all certainty, today we will finish the remaining amendments pending on the bill and hopefully finish the bill itself. A lot of these amendments have been very well-intentioned—in fact, I suspect they all have been well-intentioned—but in many cases they fundamentally undermine the core purpose of the bill, which is to have voluntary real-time sharing of cyber threats, to allow that sharing to be between private entities and the Federal Government, and even for private entities to be able to share with each other.

This is a bill that creates the liability protections and the anti-trust protections which that particular kind of sharing would allow. Of course, throughout this whole debate, there has been much discussion about how we protect our liberty in an information age. How do we have both security and liberty?

Having served for a number of years on both the House Intelligence Committee and the Senate Intelligence Committee, having served on the Armed Services Committee in the last Congress and in this Congress on the Defense Appropriations Committee, there is no argument in any of those committees that one of our great vulnerabilities is cyber security and how we protect ourselves.

We saw in the last few days that the head of the CIA had his own personal account hacked into apparently by a teenager who is in the process of sharing that information. If the head of the CIA and the head of Homeland Security do not know how to protect their own personal information, obviously information much more valuable than they might personally share is also in jeopardy.

We do need to ensure that we protect people's personal liberties. We need to do that in a way that defends the country. Both of those are primarily responsibilities that we accept when we take these jobs, and it is certainly our responsibility to the Constitution itself.

I think Chairman BURR and Vice Chairman FEINSTEIN have done a good job of bringing that balance together. This bill is carefully crafted in a way that creates a number of different layers of efforts to try to do both of those things.

First, the bill only encourages sharing; it doesn't require it. It doesn't require anybody to share anything they don't want to share, but it encourages the sharing of cyber threats. It works on the techniques and the malware used by hackers. It specifically does not authorize the sharing of personal information, and in fact the bill explicitly directs the Federal Government to develop and make available to the public guidelines to protect privacy and civil liberties in the course of sharing the information.

The Attorney General is required to review these guidelines on a regular basis. The bill mandates reports on the implementation and any privacy impacts by inspectors general and by the Privacy and Civil Liberties Oversight Board, to ensure that these threats to privacy are constantly looked at.

Senator FLAKE's amendment, which we accepted as part of the bill just a few minutes ago, guarantees that this issue has to be revisited.

I gave a speech at Westminster College in Fulton, MO, about a month ago at the beginning of the 70th year of the anniversary of Winston Churchill giving the ''Iron Curtain'' speech on that campus and talking about liberty versus security there. I said I thought one of the things we should always do is have a time that forced us as a Congress to revisit any of the laws we have looked at in recent years to be sure we protect ourselves and protect our liberty at the same time. This is a voluntary bill. Maybe that wouldn't have been quite as absolutely necessary here, but I was pleased to see that requirement again added to this bill, as it has been to other bills like this.

This is a responsible bill. The people the Presiding Officer and I work for can feel good about the responsible balance it has. It defends our security, but it also protects our liberty. I look forward to its final passage today. The debate would lead me to believe, and the votes would lead me to believe, that is going to happen, but of course we need to continue to work now to put a bill on the President's desk that does that.

There still remain things to be done. One of the things I have worked on for the last 3 years—Senator CARPER and I have worked together, Senator WARNER has been very engaged in this discussion, as has Chairman THUNE—is the protection of sensitive personal information as well as how do we protect the systems themselves.

Clearly this information sharing will help in that fight. There is no doubt about that. In addition to supporting this bill, I want to continue to work with my colleagues to see that we have a way to notify people in a consistent way when their information has been stolen.

There are at least a dozen different State laws that address how you secure personal information, and there are 47 different State laws that address how you tell people if their information has been stolen. That is too much to comply with. We need to find one standard. This patchwork of laws is a nightmare for everybody trying to comply and frankly a nightmare for citizens who get all kinds of different notices in all kinds of different ways.

Without a consistent national standard pertaining to securing information, without a consistent national standard pertaining to what happens when you have a data breach and your information is wrongly taken by someone else, we have only done part of this job. So I want us to continue to work to find the solutions there. We need to find a way to establish that standard for both data security and data breach. I am going to continue to work with the Presiding Officer and my other colleagues. Our other committee, the commerce committee, is a critical place to have that happen. I wish we could have done this on this bill. We didn't get it done on this bill, but I would say that now the first step to do what we need to do is dealing with the problem of cyber security in the way this bill does and then finish the job at some later time.

So I look forward to seeing this bill passed today. I am certainly urging my colleagues to vote for it. I think it has the protections the people we work for would want to see, and I am grateful to my colleagues for giving me a few moments here to speak.

I yield the floor.

## RECESS

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

Thereupon, the Senate, at 1:01 p.m., recessed until 2:15 p.m. and reassembled when called to order by the Presiding Officer (Mr. PORTMAN).

## CYBERSECURITY INFORMATION SHARING ACT OF 2015—Continued

The PRESIDING OFFICER. Under the previous order, the time until 4

p.m. is equally divided in the usual form.

The Senator from Rhode Island.

Mr. REED. Mr. President, I wish to comment briefly on the Cybersecurity Information Sharing Act that the Senate is considering. Let me first commend the sponsors, Senator BURR and Senator FEINSTEIN, for their extraordinary work.

This bill will help ensure greater sharing of cyber threat information, more rapidly and broadly, across industry and government. As we have seen with large-scale attacks against the Federal Government and companies such as Sony, there is an urgent need to start addressing these breaches. While such legislation is not going to eliminate our cyber security challenges, it should materially help to defeat and deter cyber attacks and assist law enforcement in tracking down and prosecuting cyber criminals. Information sharing will also assist the intelligence agencies and law enforcement to detect and trace the attacks originating from foreign actors, which is a crucial step in holding other countries accountable.

Many of our citizens and corporations are understandably concerned about the impact of information sharing on privacy. But we also must recognize that rampant cyber crime is a monumental threat to the privacy of the American people, and that sharing information about these criminal acts cannot only protect privacy but also protect our public safety and national security.

With respect to the specific privacy protections in the legislation before us, the managers of this bill have come a long way toward improving the balance between security and privacy protection, especially the changes made to the base bill by the managers' substitute.

A major area of concern was whether the government should be authorized to use information shared under this bill to investigate or prosecute a host of crimes unrelated to cyber security. Now the bill is more narrowly tailored and focused on using information gathered under this bill to go after crimes that are specifically related to cyber security.

The managers' substitute also adds a requirement that the information sharing procedures, required to be issued under this bill, include a duty to notify individuals when the Federal Government shares their personally identifiable information, or PII, erroneously.

The managers' substitute also includes an improved reporting requirement that will show the number of notices sent because the government improperly shared an individual's PII and the number of cyber threat indicators shared automatically and, in addition, the number of times these indicators were used to prosecute crimes.

So the managers' substitute has come a long way toward being more protective of individual privacy, and I would like, once again, to recognize Senators FEINSTEIN and BURR's hard work here and their willingness to listen to their colleagues. While I might personally have set the balance slightly different in some places, which is why I have supported some of the amendments before us, I think they have done a significant job in improving the bill and providing privacy protection.

I do want to draw my colleagues' attention to one important additional fact here, which in some cases has been largely overlooked. The cyber information sharing system established by this bill will require Federal dollars to implement. Many of the agencies involved—the Department of Homeland Security being the primary portal for shared threat indicators—are funded on the nondefense discretionary side of the ledger. This is an example of why I and many of my colleagues have been urging for sequester relief for both defense and nondefense spending—because we cannot defend our homeland without funding nondefense agencies such as the Department of Homeland Security and a host of other key Federal agencies. Indeed, I am encouraged that we are close to voting on a budget solution that will provide 2 years of sequester relief on a proportionally equal basis for defense and nondefense spending, and that protects the full faith and credit of the United States by taking the threat of default off the table until March of 2017.

For this reason, I look forward to final passage of this legislation. I once again commend the principal authors, Senator BURR and Senator FEINSTEIN, for their extraordinary effort.

I yield the floor.

The PRESIDING OFFICER. The Senator from Delaware.

AMENDMENT NO. 2581, AS MODIFIED

Mr. CARPER. Mr. President, I want to go back in time a little more than 12, 13 or 14 years ago, to 9/11. One of the lessons learned by the committee on which the Presiding Officer and I serve, now the Homeland Security and Governmental Affairs Committee, was learned from former Governor Tom Kean of New Jersey, cochair, along with former Congressman Lee Hamilton from Indiana, former chair of the House Foreign Affairs Committee. They were the cochairs of the 9/11 Commission. One of the things they brought to our committee and to the Congress, after a lot of work by a number of good men and women who served on that commission, was the root causes for how that disaster occurred: How could those four aircraft take down the Twin Towers, crash into the Pentagon, and crash into a field in Shanksville, PA, instead of this building right here? How could that have happened?

There are a number of reasons why it happened. But one of the reasons why it happened is that we had stovepiped our intelligence services. What the folks over at the FBI knew wasn't necessarily known or shared with the Department of Homeland Security. What the folks at the National Security Agency knew was not shared with either of the other two agencies. What the Defense Information Agency knew or what other agencies knew simply didn't get shared—stovepiped—because we did a lousy job of sharing the real story, the full truth on what was being plotted, what was going to come down and literally take thousands of lives in one day and change in many ways our country—in profound ways that still exist today. ''Stovepiping''—I have heard that word a hundred times in hearings and before our committee and in talking to folks in the 9/11 Commission. The legislation that we passed on the heels of that disaster was designed to make sure we didn't end up stovepiping again with intelligence information that might lead us to avert that kind of disaster. So far, it seems to be working and is much needed, and I think it has been helpful.

Today, I want to talk about a different kind of stovepiping that I am afraid we may end up with—not to avert or block an aviation takeover of an aircraft and disasters involving the aviation sector but a disaster in cyber space in the face of cyber threats to our country.

We are working here today and will be voting later today on an amendment or two and then on final passage of the Cybersecurity Information Sharing Act. Again, just to remind everybody, the reason why we are considering this is there needs to be a better sharing of information when businesses come under cyber attack from those within our country, outside of our country, cyber nations, and criminal organizations. We need to do a better job of sharing that information—business to business and business to government—and for the government to share that information within the government to agencies that need to know so we can respond to those attacks.

Shortly after the 9/11 Commission recommendations were enacted, one of the things that we did was we stood up a new department called the Department of Homeland Security. It is a civilian agency, as we know. It is not the Department of Defense. It is not the Department of Justice. It is not the FBI, and it is not the National Security Agency. It is a civilian organization.

When the Department of Homeland Security was created, one of the ideas behind it was that it would not be just a civilian operation, but it would be a civilian operation that could receive, from businesses and from other governmental entities, information relating to cyber attacks. That information could come through a portal—think about it; almost like a window—through which those threat indicators would be reported. Those threat indicators would come through that portal at the Department of Homeland Security. The Department of Homeland Security

would do, almost in real time, a privacy scrub to strip off from the information—the threat indicators submitted from other businesses or other government entities—Social Security numbers or other personally identifiable information or information that just shouldn't go to other Federal agencies or other businesses. They would strip it out—not in a week, not in a day, not in an hour, not even, in many cases, in a minute, but just like that—immediately—real-time privacy scrub.

As the Presiding Officer knows, we tried for years to be able to enact legislation that incentivizes businesses that have been victims of cyber attacks to share that information with one another, with other businesses, and with the Federal Government. A bunch of them have been reluctant to do it. Some of them have been reluctant to do it because they don't want to get sued. If they disclose that they had a breach and maybe their competitors didn't, how would that be used against them? How could they be named in lawsuits if attacks occurred?

So in order to get them to be willing to share information, we had to incent them. And the way we decided to incent them is to say: Share the information. You don't have to worry if you share it with the Department of Homeland Security through the portal established in this civilian agency. Share it with the Department of Homeland Security, and you have liability protection or, as it turns out, if you already shared it previously, if it has been shared previously with the Federal Government, you can share it again and still enjoy liability protection. You can share it with companies that are victims of cyber attacks, share it with their regulator, and still enjoy liability protection.

What we want to do is to make sure companies and businesses that are hacked don't just sit on the information, that they do something with it. This is a saying we have on Amtrak: If you see something, say something. If something happens to a business—a cyber attack intrusion—we want them to share it so other businesses and other Federal agencies can be prepared for it, look out for it, and stop it.

Where does this take me? This takes me to an amendment that we are going to be voting on later this afternoon offered by one of our colleagues, Senator COTTON. It would, I fear, risk revisiting stovepiping—not the kind of stovepiping that led to the disaster of 9/11 but stovepiping that could lead to cyber threats—threat indicators shared with the Federal Government but not with the Department of Homeland Security, which receives these threats and immediately disburses them to other agencies that have a need to know. But what the Cotton amendment would do is that it would say that a business that is a victim of a cyber attack could share with the FBI, could share with Secret Service, but wouldn't have to share with the Department of Homeland Security.

The reason why in our legislation, which Senator BURR, Senator FEINSTEIN, I, and others have worked on, we have it going through the Department of Homeland Security is because, more than any Federal agency, they are set up to do privacy scrubs. That is one of the things they do, and, frankly, they do it really well. Their job is to then spread that information and share that information back to the private sector, in some cases, and in other cases, just with relevant agencies—NSA, FBI, Department of Justice, Treasury, whoever else needs to know that information.

As part of the authors of the legislation, I join them in this. Our fear is if the information isn't shared with the Department of Homeland Security, which will then broadly share it in real-time and share that information with those who need to know it, and if it ends up that the FBI or, frankly, any other agency that doesn't have that ability to do a great privacy scrub maybe, that doesn't have maybe the mission to immediately share that information in real time to other relevant players, then the news—the word about that cyber attack—could literally stay at that agency—the FBI or the Secret Service, for that matter. We don't want that to happen. We don't want to see that information stovepiped in one agency. We want to make sure that it goes to one agency that does the privacy scrub. We want to make sure the agency that does the privacy scrub shares that information in real time with relevant Federal agencies and the private sector.

I probably shouldn't pretend to speak for Senator FEINSTEIN and Senator BURR. They will be here to speak for themselves. But I know they share my concerns about this legislation. I ask, on behalf of them, and, frankly, for others of us who believe that this is a dangerous amendment—and I don't say that lightly. We have worked really hard. We have worked really well across the aisle—literally for months now—to get to this point. To use a football analogy, we are not just in the red zone passing this legislation; we are on the 10-yard line, and it is first down and goal to go. Let's not muff the play. Let's get the ball to the end zone. Let's pass this legislation. Let's vote down the Cotton amendment, and let's go to conference. Let's go to conference and provide the kind of protection against cyber attacks that this country desperately needs and deserves.

I yield the floor.

The PRESIDING OFFICER. The Senator from West Virginia.

CARBON REGULATIONS

Mrs. CAPITO. Mr. President, today I rise on behalf of West Virginian workers, families, communities, and all hardworking Americans who will bear the burden of these onerous carbon mandates. The bipartisan resolution of disapproval, which I have introduced with my colleague Senator HEIDI HEITKAMP from North Dakota and 47 other cosponsors, will block EPA's greenhouse gas regulation targeting existing power sources. I also strongly support Leader MCCONNELL's companion resolution to block the regulations targeting new power limits.

As I was thinking about the speech today and as I rise to give this speech, I realize I have said many of these same words so many times before. I have expressed the same frustrations and spouted off similar statistics. What is the difference this time? The difference is we have already seen the devastating effects and the callous nature of regulatory overreach. We know what the new reality would be. The new reality would be what we are facing with these new carbon regulations: the reality of the families, the faces, and the hardships that we have already endured; the thousands of layoffs in my State of West Virginia that have already been issued; the jobs that have been lost and will never come back.

Just this morning, nearly 200 West Virginia coal miners in Randolph County were informed that their jobs will be gone by Christmas. Think about how those families will spend their Christmas holiday. Then consider how those realities will be magnified and felt throughout many households across the country if these carbon mandates move forward—the higher electricity bills that will result, the squeeze that already is squeezing struggling middle-class families who are living on fixed incomes, and the squeeze that those who live on fixed incomes will feel. Our most vulnerable will bear the burden. Consider the far-reaching effects these regulations will have on schools that are now seeing their budgets shrink, home values that are now on the decline, and fewer dollars that are available for public safety and law enforcement.

It is reality that the policies emanating from this government—from our government—are causing this destruction. This is not a natural disaster. This is not a fiscal crisis. This is not an uncontrollable event but a carefully crafted, precise, and very meditated assault on certain areas of the country. These are policies that help some States and truly hurt others, policies that target States like West Virginia and North Dakota where we produce some of the most reliable and affordable energy, and policies that are ripping the American dream away from families in my State and communities. Our families want and deserve healthy, clean air and water, and they want to live in a great environment. But policies from Washington that pit one State against another and prioritize certain communities and certain jobs over others are bringing the livelihoods of many to a halt. On behalf of Americans across the country, Members of Congress now have the opportunity to express our concerns with these carbon mandates. We have an opportunity to weigh in about whether these burdensome regulations should go into effect.

I believe that a majority of my colleagues understand the need for affordable and reliable energy, and that is why I am confident that Congress will pass these resolutions and place this critical issue of America's economic future squarely on President Obama's desk. With the international climate negotiations in Paris scheduled for December, the world is watching whether the United States will foolishly move forward with regulations that will do virtually nothing to protect our environment and will tie one hand behind our back economically. Even if the President vetoes these resolutions—and we recognize the likelihood that he will—passing them will send a clear message to the world that the American people do not stand behind the President's efforts to address climate change with economically catastrophic regulations.

I am pleased to be joined by several colleagues on the floor who understand the need for affordable and reliable energy. I would like to recognize Senator HEITKAMP.

I ask unanimous consent to engage in a colloquy with my colleagues for up to 30 minutes.

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

Ms. HEITKAMP. Thank you, Mr. President, and thank you to my great colleague from the great State of West Virginia, a State that has been powering America for many years—in fact, from the very beginning. My thanks go to all of the great workers and coal miners in her State who have added to our economic opportunity, not just for the people in West Virginia but for the people of an entire region.

That is one thing we forget—that in America a great miracle happens every day. We turn on a light switch and the lights come on. If that doesn't happen or if it is too expensive to turn on that light switch, we will not be the country that we are. With this regulation, I think what we have done is cede the all-important role of electrical security and energy security to an environmental agency that does not have the experience or expertise to understand what it takes to get an electron in the wire.

I am proud to stand today with my colleague Senator CAPITO and introduce a bill to roll back the EPA rule on carbon emissions—that rule which threatens the supply of abundant, affordable, and reliable electricity in North Dakota. I pledge to register my displeasure through multiple channels. This legislation today is the most public way of expressing not just my frustration but the frustration and concern of my State regulators and my State utilities.

Although this rule will have dramatic consequences across the country, it unfairly targets North Dakota utilities. During the original draft rule, North Dakota's allocation was 11 percent. This is not something we were happy with given the extent of the jurisdictional reach but something that people started rolling up their sleeves saying if we have to reduce by 11 percent, how are we going to do it and how are we going to meet this challenge? That is the North Dakota way, to not only fight for our rights but also look at what the alternatives are. Unfortunately, when the draft rule went from an 11-percent to a 45-percent reduction in the final rule, that was the straw that broke the camel's back.

I am trying to do everything I can to push back against EPA's burdensome powerplant rules to find workable solutions so North Dakotans can continue to have low-cost, reliable electricity. This CRA is one of the many different avenues I am taking to make sure that North Dakota is treated fairly.

I want to talk about what is unique about North Dakota. In fact, a lot of the generation that happens in North Dakota is generation that is generated by rural electric co-ops. These co-ops own and operate about 90 percent of the State's coal-based generation facilities, and they provide electricity to rural areas that in the past other utilities would not serve, not just rural areas in North Dakota but rural areas all through the region. These are people at the end of the line, as we call them, the very people that this rule will most impact and that EPA and this administration failed to consider when they made this final rule.

North Dakota's utilities are heavily invested in coal-based generation for a good and historic reason. I think this is an important point to make because a lot of people may say: Well, what is the difference? You can fuel switch. But at the time our electric co-ops built these generation facilities, they used coal because it was against Federal law to use natural gas. The fuel use act made it illegal to use natural gas for power generation, virtually forcing these power companies to make the investment that they made in this fuel source of coal. Now, after making billions of dollars of investments to meet the mandates under the fuel use act and to meet the numerous emissions standards that have been put forth by EPA, the administration once again is straining these assets, causing them in many cases to be stranded. If the administration were willing to pay fair market value to strand these assets, then maybe we could have a discussion, but I don't see that deal on the table. These utilities built, modified, and retrofitted all at great cost and according to Federal law at the time, and now they are threatening the very existence of this generation.

These assets are not just critical to North Dakota. Our coal-based generation provides dependable, affordable, reliable baseload electricity to millions of people in the Great Plains with roughly 55 percent of electric power generated in North Dakota being shipped outside our border.

When this final rule came out, I simply said that it was a slap in the face to our utilities and our regulators. This final rule was so vastly different from the rule that was proposed, it was almost laughable that EPA said it wasn't in any way informed by any real input or any real comment. How can you take a utility and a State from 11 percent to 45 percent and not reissue that rule? How can that be the movement in the final rule?

I think this final rule is a rule that jeopardizes close to 17,000 good-paying jobs in my State. It provides power for rural communities that otherwise would struggle for affordable, reliable baseload power. We have some of the lowest power costs in the country because we have some of the best utilities in the country, which are always looking out for the consumer at the end of the line.

North Dakota has never stepped down from a tough challenge, especially when the challenge is fair, the goal is attainable, and the timeline is achievable, but that is not this rule. The goal is not fair, the challenge is not fair, the goal is not attainable, and the timeline is unachievable in my State—unachievable. That is not anything the Clean Air Act ever anticipated—that we would set a goal with no feasible or possible way of meeting that goal, given current technology. Yet that is the position we are in.

At the end of the day, what matters most is making sure that our utilities can do their jobs, making sure that when a North Dakotan or a South Dakotan or someone from Wyoming or Colorado, where we deliver power—and certainly those in Minnesota—reaches over to turn on that light switch, regardless of the time of the day, that light comes on. That is called baseload power. People who think this is easy, people who think this is just switch fuels or switch technology, have never sat in a boardroom as I have and listened to the challenges of putting that electron on that wire.

I stand with my colleague from West Virginia and my colleague JOE MANCHIN here on our side of the aisle saying enough is enough. This is a problem we need to address. Maybe that is the difference in how we look at this. This is an issue that we can tackle and achieve results over time, but this rule is wrong. It is wrongheaded. It will, in fact, cause huge disruption to the economy of my State and the economy of the middle of this country. We have to do everything we can to prevent this rule from becoming a reality.

Thank you for letting me join you, the great Senator from West Virginia. We have two great Senators from West Virginia here.

I yield the floor.

The PRESIDING OFFICER. The majority leader.

Mr. MCCONNELL. Mr. President, there is a war on coal in America—a war on coal in America. The leader is the President of the United States. A number of us were in the Senate in 2009 and 2010, and the administration

couldn't pass their cap-and-trade proposal through the Senate. They had 60 votes in the Senate. The President and his party had 60 votes in the Senate, but they couldn't pass the cap-and-trade proposal through this body, so they decided they were going to do it anyway. They decided they were going to do it anyway.

As the two Senators from West Virginia can attest, we have a depression in central Appalachia, created not because of anything we did here in Congress but because of the President's zeal to have an impact worldwide on the issue of climate. I suspect that even if we follow this path all the way to the end, this effort by the United States would have about as much impact as dropping a pebble in the ocean. Yet we are paying a real price for it here at home. Eastern Kentucky looks like the Dust Bowl during the thirties—no jobs, no opportunity, no future, not as a result of anything we passed through the people's elected representatives but by this sort of arrogant, singlehanded messianic goal to deal with worldwide climate.

Our options to stop it are quite limited. We do have the possibility of the Congressional Review Act, but the weakness of that obviously is that even though we can pass it with a simple majority, he is likely to veto it.

We are here today to stand up for our people, the ratepayers of America, and not only the ratepayers—90 percent of the electricity in Kentucky comes from coal—but the communities that have been devastated by this. I have never seen anything like it. I heard my parents talk about what the Depression was like. It sounds and looks a lot like the stories they told me about America in the 1930s.

This is a venture that will have no impact on the issue for which it is being pursued but is having a devastating and current adverse impact on the people we represent.

We have representatives from both parties here on the floor today working toward overturning the administration's deeply regressive energy regulations. These regulations are going to ship more middle-class jobs overseas. I told my constituents last year: Coal has a future; the question is, Does coal have a future in this country? The Indians and the Chinese are not going to give up their future by not using this cheap and abundant source of power. The Germans—one of the greenest countries in Europe—are now importing coal. So coal has a future. The question is, Does it have a future here after this administration?

My folks can't even put food on the table. The ones who can find a job somewhere are leaving. The population continues to decline.

As I said earlier, it is not going to have much of an impact on the environment of our planet. This isn't going to do anything meaningful to affect global carbon levels. It just seems that someone wants to be able to pat themselves on the back for doing something even if they accomplish hardly anything at all, except hurt a whole lot of Americans. Higher energy bills and lost jobs may be trivial to some folks out on the political left—not their jobs; they don't care—but it is a different story for the middle-class Kentuckians whom I represent.

So here we have on the floor Senators from both parties who are saying it is time to take off the ideological blinders and instead think about those who have already suffered enough over the past few years. We have worked together to file bipartisan measures that would overturn the administration's two-pronged regulations. I have joined with Senator HEITKAMP and Senator CAPITO on a measure that would address one of those prongs, the one that pertains to existing energy sources. Senator MANCHIN is here on the floor and joined me as I introduced a measure that would address the other prong, the one that pertains to new sources. These bipartisan measures together represent a comprehensive solution. As I said, I am pleased to be joined here on the floor by Senators from West Virginia and North Dakota. Senator DAINES from Montana is here—another important coal State. The chairman of our Environment and Public Works Committee, Senator INHOFE, is here, and some have already spoken and some will speak after me. I am proud and pleased to be here on the floor with all of my colleagues standing up for our aggrieved constituents who have been mightily abused by this administration.

I yield the floor.

The PRESIDING OFFICER (Mr. PERDUE). The Senator from West Virginia.

Mr. MANCHIN. Mr. President, first of all, I want to thank my colleagues, Senator MCCONNELL, Senator CAPITO, who is my colleague from the State of West Virginia, Senator DAINES, Senator INHOFE, and my good friend Senator HEITKAMP.

This is a bipartisan approach. Not often do we see a bipartisan effort, a bipartisan colloquy on the floor of the Senate anymore, and there should be because we all have the same interests. Basically, how do we provide affordable, dependable, and reliable energy? That is what this country was built on. We have defended this country by having resources that we could use to basically defend ourselves, and that resource has come from what the Good Lord gave us. Coal has been in abundance in the United States of America. We have fought every war, we have defended, we have energized, and we have built a middle class unlike at any time in the history of this world.

So now it comes to the point where there is a group—basically the ones on an ideological pathway—who says we can do it differently. If someone came to me and said: We have this new great energy, and I am sorry, West Virginia and North Dakota and Oklahoma and Montana, we have this new energy—and maybe it is commercial hydrogen, which will be water vapor—that is wonderful. We will figure a way. We will embrace that. We will figure a way to make it. We will do something. We will diversify. That is not the case. The case is simply this: This country has depended and will depend—even by this administration's admission, this country will depend on fossil fuel for at least the next three decades. It is in the EIA report. They are going to have to have it. Baseload, as the Senator from North Dakota said, is simply this: something that will give us power 24/7, day and night, rain or shine. There are only two things in the world that can do it: coal and nuclear. Gas is coming on and gas will be a baseload when the distribution lines and the pipelines are there to provide it. Right now it is not, but it is coming on strong.

Just look no further than Japan. Japan was mostly moving toward nuclear. Fukushima happens. When that happened, Japan had to change. What did they do? They changed to coal. But they decided the new plants they would build would be ultra super critical. That means 40 percent efficiency, burning at the highest levels to reduce the emissions. They are moving in technology ways.

Now, what does the plan that we are talking about and we have our colleagues talking about—existing source, which means they can't continue with what we have today, and new source, which means any new plant has to be built to certain standards. Carbon capture sequestration has not been proven commercially, not at one plant in America. Yet these rules are based on using carbon capture sequestration.

All we have said—some of us have said this: Why don't you at least demonstrate that you can have that type of commercial operation and that it can withstand 1 year under commercial load and show us those are the new limits you want us to meet? That, to me, is reasonable.

Let me tell my colleagues this: If you were in the business of producing power and you desired not to do that even though we had technology, then you would have to close your plant. I understand that. That is not the case. They can't show us technology and show us that it has a commercial feasible pathway to be able to perform and provide the energy we need. There is no way they can do it.

So I have said this: If it is unobtainable, it is unreasonable. That is all. Don't expect me to do something that has never been done. If the Federal Government says: Fine, we have $8 billion lying down at the Department of Energy—$8 billion that hasn't been tapped—does that not tell us something?

The private sector has not stepped up to take those types of loans and to use those types of loans to find the new technology for the future because they don't believe the administration wants

us to find any new technology that might be able to adhere to the standards they have set.

So we sat back and we have done nothing. Then, on top of that, they expect these plants, 30 years from now—if they are expecting to get commercial power, electricity, fill the grid with power coming from coal for the next 30 years—most of our plants average 50 years of age. They can't produce the power they are going to produce—that we will need for this country to have for 30 more years. An 80-year-old plant just won't do it. So that means they come off the line, off the grid. When that comes off the grid, what we call dependable, reliable, and affordable energy goes away. It goes away.

I have said this: Someone needs to respectfully ask our President, this administration, the EPA, the DOE: If for the next 90 days not another ton of coal was delivered to a coal plant in America—not another ton of coal because—and I have said this to the administration. They have been very eloquent in basically telling the American people: We don't like coal, we don't want coal, and we don't need coal. If those were the facts, then make sure you tell the American people, if they didn't have coal for 90 days, what the United States of America would look like. Just tell me what it would look like. Ask anybody what it would look like. The lives of 130 million people would be in jeopardy tomorrow—130 million people. This system could collapse. The east coast could be dark. Now, you tell me how you are going to fill that in. And if you are not willing to be honest with the American people and tell them that, don't make them believe there is something that is not there, that you can run this off of wind and solar.

We have a lot of wind in West Virginia, and we are proud of that. I will give an example. My colleagues will remember the hottest days this past summer, that very hot spell we had, 90 to 100 degrees. We have 17 acres of a wind farm on top of a beautiful mountain in West Virginia, 560 megawatts. We have a coal-fired plant sitting there, the cleanest super-critical coal-fired plant on Mount Storm, 1,600 megawatts. Guess how many megawatts of power the wind produced during the hottest times of the summer when we needed the power. Two megawatts. Two. The wind didn't blow. It was so hot and stagnant, it didn't blow. That poor little coal-fired plant was giving it everything it had to try to produce the power the Nation needed.

I am just saying the facts are the facts whether we like them or not. So when this plan comes out and says that any new coal-fired plant being built has to be—you can basically be assured they are not going to build any. When they are saying existing plants have to meet certain standards, they won't invest and try to hit a moving target.

So now what happens? For the 35 to 40 percent of the power you are telling the United States of America, the people in this great country, that we have—don't worry, we are going to take care of you, it is not going to happen. We are not going to stand by and say we are not going to fight for that. We are not only fighting for a way of life for West Virginia, we are fighting for a way of life for this country.

This country depends on energy we have been able to produce. We have always depended on our little State. North Dakota, now one of the best energy-producing States we have in the country—Montana, Wyoming, Oklahoma—we have been the heavy lifters. We will continue to work for this great country. We just need a little help. That is all we are asking for.

So I would say, ask the question: What would the country look like tomorrow? The standards they are setting are basically unreasonable, totally unreasonable, because they are unobtainable.

The impact is going to be devastating, basically. The system is going to be to the point to where we can't depend on it, it is not reliable, and we don't have the power of the future yet. Maybe our children or grandchildren might see that. I hope so. But until the time comes where we are going to transition from one to the other, make sure it is a smooth transition. Make sure it is a dependable transition. Make sure it is one that keeps this country the superpower of the world. If we don't, I guarantee we will be the last generation standing as a superpower saying that we are energy independent; we are not fighting wars around the world basically for the energy this country needs. We have the ability to basically take care of ourselves. We can be totally independent with energy if we have an energy policy that works, but it has to be realistic. This is not.

That is why I totally oppose this new power plan which is coming out. It is a shame that we have to rely on the courts to protect something we should be doing in the Halls of this Senate. It is a shame that the courts have to step in to protect us.

With that being said, I yield the floor, and I thank my colleagues for being here on this important issue.

The PRESIDING OFFICER. The Senator from Oklahoma.

Mr. INHOFE. Mr. President, first of all, I appreciate the fact that my colleagues from West Virginia, North Dakota, Kentucky, and Montana—all of us are getting together on this in a bipartisan way. I think it is worth repeating, to make sure everyone understands where we are on this, what a CRA is. The CRA is the Congressional Review Act. It is an act that allows an elected person who is answerable to the public to weigh in on these decisions that are made by the President—who can't run again for office—and by the unelected bureaucrats who are destroying this country.

As was pointed out by the Senator from Kentucky, I do chair the committee called the Environment and Public Works Committee. On this committee, we deal with these regulations. We have jurisdiction over the EPA. It is interesting I would say that because we tried to get the EPA to come in and testify as witnesses as to how the President plans to move to the percentage of power that is going to be generated by the year 2030 by renewables, and they won't testify because they don't have a plan. They don't know how they are going to do it.

The CRA is significant because there are a lot of people in this case who would be the liberals in this body who like the idea of being overregulated, who like the idea of having the regulators run our lives, and they are the ones who would love to go home when people are complaining about the cost of all of these things and they can say: Well, wait a minute. Don't blame us. That was a bureaucrat who did that; that wasn't me.

Well, this forces accountability, and these guys don't like it. I can assure you right now that we are going to give everyone an opportunity to weigh in on what these issues are. They would much prefer to go home and say: I know we are overregulating and I know it is destroying the States—whatever the States happen to be—but it wasn't me, don't look at me.

Now we are going to see who is responsible because what is going to happen is we are going to have a vote. The vote is going to take place, and I think our leader is correct when he says the President will probably veto this. If the President vetoes it, it comes back for a veto override, and then people will know who is for it and who is against it. So I think a CRA has another great value. It forces accountability by people who are answerable to the public.

On the issue we are discussing today, the interesting and the consistent pattern we have is that what this President does is he gets the things they tried to do through over—through legislation, and those things that fail through legislation he tries then to do by regulation.

Let me give you an example. Another issue—not the issue we are talking about today—is the WOTUS issue, the waters of the United States. Historically, it has been the States that have regulations over the waters except for navigable waters. Well, of course, liberals want everything in Washington. So 5 years ago a bill was introduced, and the bill would have essentially taken the word ''navigable'' out so that the Federal Government would have control over all the waters in my State of Oklahoma and throughout America. Two of them introduced a bill, one was Senator Feingold of Wisconsin and the House Member was Congressman Oberstar from one of the Northern States. I don't know which one it was. They introduced a bill to take the word ''navigable'' out. Not only did we overwhelmingly defeat the legislation, but the public defeated the two of them in the next election.

Now the President is trying to do what he was not able to do through legislation through regulation. The same thing is true—the Senator from West Virginia is right when he talked about what they are trying to do. It is very interesting when you look at this bill. We are talking about the emissions of $CO_2$. The first bill that was introduced was in 2002. It was the McCain-Lieberman bill. We defeated that. The next one was the McCain-Lieberman bill in 2005, and the third one was the Warren-Lieberman bill in 2008. Then we had the Waxman-Markey bill that we never even got to vote on because nobody was going to vote for it.

So what they fail to be able to do legislatively, they are now trying to do through regulations, and that is why a CRA is significant because it does force accountability.

Let me make one other statement. This thing about Paris that is going to take place in December. This is the big party that the United Nations puts on every year. It is the 21st year they have done this. I can remember when they did it in 2009. That was going to be Copenhagen. Several people went over there at that time. President Obama was in the Senate, Hillary was in the Senate, PELOSI was there, and John Kerry went. They went over there to tell the 192 countries that were meeting in Copenhagen—the same 192 countries that will be meeting in 2 months—went over to tell them we were going to pass cap-and-trade legislation that year. That was 2009.

I went over after they had given their testimony there. I went all the way over to Copenhagen, spent 3 hours, and came all the way back on the next flight. I probably had the most enjoyable 3 hours I ever had because I was able to talk to 192 countries and tell them they had been lied to; that we are not going to be passing it. The same thing is going on in December of this year.

By the way, let me just mention one thing that hasn't been said. There are people out there listening to this who actually believe this stuff, that the world is going to come to an end because of $CO_2$ manmade gases. This is something we have been listening to for a long period of time. I remember right before going to Copenhagen in 2009—at that time the Administrator of the Environmental Protection Agency was Lisa Jackson, an appointee by President Obama, and I asked her this question on the record, live on TV. I asked: If we had passed any of the legislation or the regulations that we are talking about passing, would this have an effect of lowering the $CO_2$ worldwide? She said—now keep in mind this was an Obama appointee—by the way, Obama was President at that time when he went to Copenhagen. She said: Well, no, it wouldn't reduce emissions worldwide because it just pertains to the United States.

This isn't where the problem is. The problem is in India, it is in China, it is in Mexico. The problem we would have there is, yes, we might lower our $CO_2$ emissions in the United States. However, those other countries will not, and it could have the effect of increasing, not decreasing, $CO_2$ emissions because as we chase our manufacturing base overseas to places they don't have any restrictions, we would have the effect of increasing it.

So I am just saying I appreciate the fact we are all together on this and making the necessary efforts to make people accountable. I think it might surprise a lot of people as to who changes their mind on this once they know they have to cast a vote and be accountable.

I applaud, certainly, my friends from West Virginia and the other States that are involved in this. I think this is the right thing to do. Let's keep in mind the Utility MACT—that is the maximum achievable control technology—was the first shock to put coal under. At that time we did a CRA, and we actually came within four votes of getting the bill passed, and that was when Republicans were not a majority. I look for some good things to happen, and I think we are doing what is right and responsible.

I yield the floor.

The PRESIDING OFFICER. The Senator from West Virginia.

Mrs. CAPITO. Mr. President, I ask unanimous consent for additional time so the Senator from Montana can join the colloquy. As he reminds me, the Senator has the largest recoverable tonnage of coal in the Nation.

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

Mr. DAINES. Thank you, Mr. President.

This administration is shutting down coal-fired powerplants in the United States. I thank the Senator from West Virginia, Mrs. CAPITO, the other Senator from West Virginia, Mr. MANCHIN, and we have Senator HEITKAMP here. We had Democrats and Republicans in colloquy talking about what is going on with coal-fired plants and the Clean Power Plan of this administration.

This is what is happening. It is killing good-paying jobs for union workers, for pipefitters, for boilermakers, and tribal members in my State with these so-called Clean Power Plan regulations. At the same time, it is stifling investment that could lead to innovation to make coal cleaner in the United States.

As I travel across Montana, I have heard Montanans describe the EPA as—a rancher once told me it stands for ''Eliminate Production Agriculture.'' A union member recently told me it stands for the ''Employment Prevention Agency.'' President Obama and his ''Employment Prevention Agency'' continues to wage war on American energy, American families, and on American jobs. This so-called Clean Power Plan is an all-out frontal assault on affordable energy and good-paying union jobs as well as tribal jobs. This will leave President Obama directly responsible for skyrocketing energy bills, a loss of tax revenue for our schools, teachers and our roads and the unemployment of thousands of hard-working Americans. The President ignores the fact that more than half of Montana's electricity comes from coal, as do thousands of jobs and $120 million in tax revenue every year.

In fact, 40 percent of our Nation's energy comes from coal. When a young person plugs their iPhone or their smartphone into the wall and charges it, most likely it is being charged by coal.

In my hometown of Bozeman, we have a Tesla charging station at one of our hotels. Elon Musk at Tesla did an amazing, innovative job creating electric vehicles, but when they plug those Tesla vehicles into those chargers, those Tesla vehicles in Montana are likely powered by coal.

The facts are that coal production in the United States is much safer and less carbon intensive than coal from other nations. As had been mentioned, this is a global challenge we must think about and address. The Powder River Basin in Southeast Montana has coal that is among the cleanest in the world. It has lower sulfur content and cleaner than Indonesian coal. Shutting down U.S. coal will have a negligible impact on global coal demand and global emissions. However, it will ultimately make it more likely that less technologically advanced coal production techniques will be used around the world.

This is the way to think about it. The United States consumes about 10 percent of the world's coal. Said another way, 90 percent of the coal consumption in the world occurs outside the United States, and the global demand for coal-fired energy will not disappear even if the United States were to shut down every last coal mine and every last coal-fired plant.

Again, individuals are entitled to their own opinions but not to their own facts. Here are the facts. Coal use around the world has grown about four times faster than renewables. There are 1,200 coal plants planned across 59 countries. About three-quarters of them will be in China and India. China consumes 4 billion tons of coal per year versus the United States at 1 billion tons. China is building a new coal-fired plant every 10 days, and that is projected to last for the next 10 years.

In Japan—I used to have an office in Tokyo. My degree was in chemical engineering, and I was part of a software company with offices around the world. I remember the big earthquake that struck Japan—the 9.0 quake. The Fukushima nuclear reactors were disabled. How is Japan dealing with that? They are building 43 coal-fired powerplants. By 2020, India may outbuild 2½ times more coal capacity as the United States is about to use. So it is shortsighted and misguided to move forward on an agenda that is going to devastate

significant parts of the economy. It is going to raise energy prices and destroy union jobs and tribal jobs.

We are seeing that already in Montana. Earlier this month, in the month of October, a customer of the Crow Tribe, the Sherco Coal plant in Minnesota announced it needs to shut down two units. This cuts off a significant portion of the customer base for Crow coal. Because the Crow Tribe relies on coal-fired Midwest utilities for most of its non-Federal revenue and for good-paying private jobs at the Absaloka Mine, the unemployment rate on the Crow reservation today is in the high 40 percent. Without these coal mining jobs, that unemployment rate will go to 80 to 85 percent.

Ironically, some of the first impacted by the Obama administration's new regulations are those who can least afford it. You have heard it from Senators on both sides of the aisle today. Under the final rule, the Colstrip powerplant in Montana will likely be shuttered, putting thousands of jobs at risk. We must take action. We need to stop these senseless rules.

This past weekend I joined the Montana attorney general, Tim Fox, in Helena to announce that Montana, along with 23 other States, has filed a lawsuit against the Federal Government because of Obama's recent decision. There are currently 26 States—the majority of the States in this United States—through three different lawsuits that have requested an initial stay on the rule.

As Leader MCCONNELL mentioned in 2010, a Democratic-controlled Congress could not pass these regulations. The people's House stopped it, but now President Obama and the EPA are moving forward without the people's consent.

I am thankful to partner with a bipartisan group of my colleagues, Leader MCCONNELL, Senator CAPITO, Senator INHOFE, Senator MANCHIN, and Senator HEITKAMP, who are speaking out and working to stop this harmful rule. I am proud to stand and join them as a cosponsor of two bipartisan resolutions of disapproval under the Congressional Review Act that would stop the EPA from imposing the anti-coal regulation.

Coal keeps the lights on, it charges our iPhones, and it will continue to power the world for decades to come. Rather than dismissing this reality, the United States should be on the cutting edge of technological advancements in energy development. We should be leading the way in using clean, affordable American energy.

America can and should power the world. We can only do it if the Obama administration steps back from the out-of-touch regulations and allows American innovation to thrive once again. In summary, we need more innovation, not more regulations.

Thank you, and I yield back my time.

The PRESIDING OFFICER. The Senator from West Virginia.

Mrs. CAPITO. Mr. President, I would like to thank my colleagues for joining me in a colloquy, particularly the Senator from North Dakota, who is cosponsoring the Congressional Review Act legislation with me on existing coal-fired powerplants, and certainly my colleague from West Virginia Senator MANCHIN. We have worked very well together in a bipartisan way on these issues—Leader MCCONNELL, Chairman INHOFE, and Senator DAINES from Montana.

I think we have presented a clear picture of the impact of these rules. So I ask unanimous consent that any time spent in a quorum call before the 4 p.m. vote series be charged equally against both sides.

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

Mrs. CAPITO. I yield the floor.

The PRESIDING OFFICER. The Senator from Florida.

PUERTO RICO

Mr. NELSON. Mr. President, I want to talk about the financial crisis that is going on in Puerto Rico. We have all heard about the current situation that Puerto Rico finds itself in. They are suffering. They are having trouble paying their bills and their economy is in shambles. Some people have the attitude ''Well, that is not our problem,'' but they are forgetting the fact that Puerto Rico is part of the United States. It is a territory. It is not a foreign country. Puerto Ricans are American citizens.

If a problem exists in Puerto Rico, it exists in the United States. It is not something we can just ignore. It impacts the entire country. If the economy continues to suffer in Puerto Rico, the people there will just move to another part of the country. I want to repeat that. If things are bad in Puerto Rico economically, they—Puerto Ricans—can move to another part of the country. This is not immigration; this is a move to the mainland. Many Puerto Ricans are leaving Puerto Rico because of it is troubles.

Happily, many of the people who live on the island are moving to Florida. They are adding to the diversity and immense fabric of Florida that reflects the entire country, but our gain in Florida is Puerto Rico's loss. There are more than 1 million people in Florida alone who may have preferred to stay at home on the island with their friends and their families. People who otherwise would be opening small businesses or new doctors' offices in San Juan are opening them in Orlando. This only hurts Puerto Rico's economic future.

We need to give Puerto Rico the tools it needs to get its economy back on track. Puerto Rico cannot do that alone. Congress needs to pitch in. I have joined a number of our colleagues—BLUMENTHAL, SCHUMER, and MENENDEZ—in being a sponsor of the Puerto Rico Chapter 9 Uniformity Act. It fixes a glitch in the Federal bankruptcy law that stops Puerto Rico's municipalities and public corporations from restructuring their debt through the Federal bankruptcy court, something that is law in all of the States. That is why we have a bankruptcy law, but there is a glitch that you cannot do that in Puerto Rico. That is simply unfair. The people of Puerto Rico should get equal protection under the law.

Both the Finance Committee and the Energy and Natural Resources Committee have held hearings in the past few weeks about the economic crisis in Puerto Rico. Two of Puerto Rico's elected officials, Governor Garcia Padilla and Congressman PIERLUISI, have testified at these hearings. Both said that Puerto Rican public corporations need access to Chapter 9 debt restructuring.

It is this Senator's strong desire that we see them treated equally under the law and that this legislation to fix this glitch comes to the floor soon. We also need to help Puerto Rico's health care system. The Medicaid Program in Puerto Rico serves nearly 1.7 million residents. It is in terrible shape. In 2010, Congress passed the Affordable Care Act, which provided Puerto Rico with a $5.4 billion one-time payment to cover health care costs. That money is set to expire in 2019, but it could even run out sooner.

Under Medicare Part D, Puerto Rican residents are being treated like second-class citizens. They don't get the same financial support that State residents get for prescription drug coverage. This has an effect on their economy, stifling their ability to emerge from the crisis, not to speak of the fact that they are not getting the health care other American citizens have.

I remind you, Puerto Ricans are American citizens. So this kind of treatment under Medicare flies in the face of the most basic American value—equality. That is why several of us have joined Senator SCHUMER on a bill to improve the way Puerto Rico is treated under Medicare and Medicaid.

Last week, thankfully, the White House released a set of legislative proposals to help Puerto Rico. Included in that list were some of the bills I have mentioned here that I support. I urge our colleagues to give this problem the attention it demands. We should move the proposals that we can move in this legislative body. We should do it with haste. There are more than 3½ million people in Puerto Rico. They are U.S. citizens who, unlike most U.S. citizens, have no one to represent them in this Chamber and only have a nonvoting delegate in the House of Representatives. They have no voice here, but even with no voice, there are some of us in this Chamber who will make sure that their voice is heard. We cannot turn our backs on fellow Americans. By the way, when it comes time to defend this country and our national security, look at the percentage of Puerto Ricans who sign up for the military. They are fellow Americans. I ask my colleagues to look deep in their hearts

and find a way to come together to help the island of Puerto Rico, a territory, our fellow American citizens, to get through this troubled time.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

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

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

BUDGET AGREEMENT

Mr. NELSON. Mr. President, since I see no one is waiting to speak, I might offer a couple of comments about the proposed budget agreement. We are still evaluating this, looking at the details, but first things first. This seems to me to be something we should agree to. It certainly gets us past this artificial debt crisis that would cause the United States to go into economic cataclysmic fits.

If we do not raise the debt ceiling, America cannot pay its obligations it has already incurred. It would be the first time the U.S. Government went into default. That time has already run out, but through extraordinary measures the Secretary of the Treasury has been able to keep the cashflow going, but he is running out of all of his tricks of the trade next week, November 3. That is the first thing it would do most immediately.

The second thing it would do is it would get us over this budgetary impasse of a budget that lays out the blueprint—for the flushing out of that blueprint, which are the appropriations bills. So in the case of the budget, what had been brought forth was a budgetary gimmick of saying we were going to raise the amount of money we needed for defense, but it was not going to meet this arbitrary budget cap that had been set 3 years ago by the cuts across the board called the sequester. But oh, by the way, we were going to increase that defense spending a little more by creating an additional account over and above what we spend overseas called the overseas contingency fund, OCO, and therefore money was going to be supplied—the increases we need in defense—with in fact not increasing the budgetary caps on spending.

Well, that was budgetary fakery. That was budgetary sleight of hand. That was not budgetary truth. This agreement stops that for the next 2 years. Two years from now we will have to face the same thing and get rid of this artificial cut across the board. That is no way of dealing with trying to cut the budget. You ought to be cutting the budget with a scalpel, not with a meat cleaver, where you come across the board on every program.

Indeed, what this agreement does is it raises the caps on defense in this first year $25 billion. It allows an OCO increase of $23 billion—and that is considerably less than what had been proposed earlier. Indeed, as you get into fiscal year 2017, it raises the budgetary caps on defense by $15 billion, also a $23 billion OCO, or overseas contingency fund, for the war effort over in Central Asia.

This is a good program, but the other thing this agreement corrects—in the Republican budget, they had only raised money for defense spending, and all the other needs of government that need to be appropriated—nondefense discretionary spending—were kept artificially low. If you are talking about grants from NIH, that was all being limited. If you are talking about money for NASA as we get into the program of going to Mars, all of that had been cut. If you are talking about agricultural programs, all of that had been cut. No matter what program—education, the environment, you go on down the list—all of that had been cut.

This budget agreement that we will vote on hopefully in the next 2 or 3 days does, in fact, raise those budgetary caps for nondefense spending as well as for defense spending. So where the caps were raised in this first year of fiscal year 2016 by $25 billion for defense spending, so too $25 billion for nondefense discretionary spending. Likewise, in the next fiscal year, 2017, where the caps had been raised $15 billion for defense spending, likewise, nondefense discretionary and all those other needs of government, the same amount—$15 billion.

I will have more to say about this later, but while I have the opportunity, I wish to commend to the Senate that I think it is certainly in the interests off of our country to move forward and approve this new budgetary agreement.

By the way, I might add as I close that an agreement has been hammered out between the Republican and the Democratic leadership in both Houses, along with the White House.

I yield the floor.

Mr. LEAHY. Mr. President, in today's digital age, many Americans live their lives online. We communicate via email, use photo sharing and social networking Web sites, store documents in the cloud, and access our private financial and medical information through the Internet. The amount of sensitive electronic data that we create and store on the Internet is staggering and will only continue to grow. We know that cyber security is an important component of protecting our critical infrastructure. A cyber attack targeting the electric grid in the Northeast, for example, could have dire effects during a cold Vermont winter. I know that Vermonters care about cyber security, and Congress must act responsibly to strengthen our ability to defend against cyber attacks and breaches. But I also know that Vermonters care deeply about their privacy and civil liberties, and I believe just as strongly that whatever Congress does in the name of cyber security must not inadvertently undermine the privacy and security of Vermonters and all Americans.

For years, Congress has seemed singularly focused on the private sector's desire for voluntary information sharing legislation. While improving the flow of cyber threat information between the government and private sector is a laudable goal that I support, it is not a panacea for our cyber security problems. Information sharing alone would not have prevented the major breaches of the past year, such as the breach at the Office of Personnel Management, OPM, or the breaches at Sony, Home Depot, or Anthem.

Narrowly tailored legislation to facilitate the sharing of technical, cyber threat data could be beneficial, but the Senate Intelligence Committee's bill lacks certain basic safeguards and threatens to significantly harm Americans' privacy. That is why I have heard from a number of Vermonters who oppose the bill and that is why consumer advocacy organizations, privacy and civil liberties groups, and major technology companies like Apple, Dropbox, and Twitter all vocally oppose the bill. The technology companies know firsthand the importance of ensuring our cyber security, and they oppose this bill because they believe it does little to improve our cyber security and would ultimately undermine their users' privacy.

For months, I have worked with Senator FEINSTEIN to improve this bill. She has been receptive to my concerns, and I appreciate that many of the revisions that I suggested are now incorporated into the managers' amendment. The managers' amendment now makes clear that companies can only share information for cyber security purposes, which is an improvement from the original legislation. It also prohibits the government from using information shared by private companies to investigate routine crimes that have nothing to do with cyber security. And it removes a completely unnecessary and destructive new exemption to the Freedom of Information Act, FOIA, which had the potential to greatly restrict government transparency. These are significant improvements, and I am thankful to Senator FEINSTEIN for working with me to incorporate them into the bill.

Unfortunately, the Senate Intelligence Committee's bill still has major flaws. This bill overrides all existing legal restrictions to allow an unprecedented amount of data—including Americans' personal information—to flow to the government without adequate controls and restrictions. It needlessly requires all information shared with the government to be immediately disseminated to a host of Federal agencies, including to the NSA. It fails to adequately require companies to remove irrelevant personal information before sharing with the government. The bill contains broad authorizations that allow companies to monitor traffic on their networks with liability protection and employ ''defensive measures'' that may

cause collateral harm to innocent Internet users. The bill also continues to include another unnecessary FOIA exemption that will weaken the existing FOIA framework.

Proponents of the bill have attempted to assuage many of these concerns by arguing that sharing under this bill is voluntary, and if companies do not want to share information with the government or use the authorities in the bill, they do not have to. This bill may be voluntary for companies, but it is not voluntary for consumers. American consumers have no say on whether their information is shared with the government and ends up in an NSA or IRS database. They may have no recourse if a company needlessly monitors their Internet activity or inappropriately shares their personal information with the government.

Rather than limiting the dissemination of information in order to protect the private and proprietary information of Americans and American businesses, this bill goes in the wrong direction by giving companies more liability protection and more leeway on how to share our information. The most effective action Congress can take to improve our cyber security is to pass legislation that requires companies to take greater care of how they use and protect our data, not less. And we should pass my Consumer Privacy Protection Act to require companies to protect our personal information and help prevent breaches in the first place. The cyber security legislation before us today does nothing to address this very real concern, so I cannot support it. I fear that this bill will significantly undermine our privacy, and I urge Senators to vote against passage.

The PRESIDING OFFICER. The Senator from Arkansas.

Mr. COTTON. Mr. President, I ask unanimous consent to speak for up to 15 minutes.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

AMENDMENT NO. 2581, AS MODIFIED

Mr. COTTON. Mr. President, today I speak in support of the Cotton amendment to the Cybersecurity Information Sharing Act. My amendment is straightforward. It simply would provide liability protection to any business or other private organization that shares cyber threat indicators to the FBI or the Secret Service.

In its current form, the Cybersecurity Information Sharing Act would require entities to submit these cyber threat indicators through a portal created and run by the Department of Homeland Security in order to receive liability protection. But there are also two exceptions that would allow entities to receive liability protection outside the DHS portal: first, if a submission was related to a previously shared cyber threat indicator, and second, if the submitting entity is sharing information with its Federal regulatory authority. But not every private entity has a Federal regulatory authority, thank goodness, so where a cable company can share with the FCC or an energy company can go to the Department of Energy or FERC, other businesses are forced to go to the DHS portal. Good examples are retailers such as JCPenney, Walmart, Target, and Home Depot.

When the trade associations for two victims of the biggest cyber attacks in recent memory—Target and Home Depot—are pleading for this language, we should take notice and incorporate it. Anything else would be unfair, inequitable, and unwise.

We ought to give these companies an alternative to the DHS portal. One simple reason is that nobody knows what the portal will look like, how it will function, or how much it will cost companies to interact with it. The Federal Government, after all, doesn't have the best track record for designing and deploying IT systems. Healthcare.gov was not exactly a resounding success. One could easily imagine a company trying to share a cyber threat indicator and getting an error message from the portal, just as millions of Americans received when they tried to sign up for ObamaCare.

In this case, regulated businesses can just go to their regulator. Private and small businesses will be out of luck, though. This is the primary reason my amendment has such strong private support. Organizations such as the National Retail Federation, the chamber of commerce, the National Cable & Telecommunications Association, and many others support this commonsense amendment.

The second main reason that entities should be able to share directly with the FBI and the Secret Service is that the bill is about promoting collaboration between the government and the private sector, as the National Security Council says that we should in this tweet: ''More than any other national security topic, effective cybersecurity requires the US gov't & private sector to work together.'' I agree.

As Director Comey recently told the Senate Intelligence Committee, the FBI has redoubled its efforts to reach out to private businesses in this area. This has paid dividends. And there is no entity in the Federal Government that the private sector trusts more on cyber security than the FBI. That is why Sony Pictures called the FBI when it was hacked by North Koreans last year.

I also have to imagine that is the main reason the White House endorsed my amendment over the weekend when they sent out this very helpful tweet: ''If you are a victim of a major cyber incident, a call to @FBI, @SecretService, or @DHSgov is a call to all.'' My goodness, Susan Rice and I stand together in agreement that if you are a victim of a cyber incident, you should be able to call the FBI, the Secret Service, or the DHS. I thank the National Security Advisor and the White House for their support for the concept behind my amendment.

I would also like to take a few moments to dispel a few myths about this amendment. The first myth is that the Cybersecurity Information Sharing Act creates a single portal at DHS for liability-protected information sharing with the Federal Government and that the Cotton amendment would create an unprecedented second channel.

This is false. The bill authorizes multiple liability-protected sharing channels with the Federal Government, not just one, through a broad exception to the DHS portal that permits certain regulated businesses to engage in liability-protected sharing of cyber threat information directly with any Federal regulators without requiring that it first pass through DHS. The Cotton amendment simply provides the same flexibility for businesses that already have established threat-sharing relationships with the FBI or the Secret Service to maintain their existing channels for sharing and not incur significant costs and delays to establish new ones with DHS. My amendment is consistent with this multichannel sharing approach.

The second myth is that my amendment would harm privacy as it would allow the sharing of cyber threat indicators with the FBI and the Secret Service and that the sharing with these agencies wouldn't happen under the bill in its current form.

This is also false. Under the current version of the bill, if an entity shares information through the DHS portal, the FBI and Secret Service will receive it. My amendment doesn't change that or the privacy protections in the bill. Both with and without my amendment, the FBI and Secret Service will get cyber threat indicators.

The third myth is that the scrub DHS would have to conduct for personally identifiable information is not as rigorous under my amendment.

Again, this is not true. The Cybersecurity Information Sharing Act requires all Federal entities receiving threat indicators to protect privacy by removing personal information that may still be contained in them before sharing with other entities. My amendment does not eliminate or weaken any of the bill's privacy requirements, as the FBI and Secret Service are required to protect privacy in the same way all other Federal entities receiving threat indicators.

Finally, I simply want to note that the House-passed version of the bill contains a nearly identical provision, and that bill passed with overwhelming bipartisan support on a 307-to-116 vote.

To sum up, the Cotton amendment has overwhelming support in the private sector, including companies that have been victims of cyber crimes. It would lead to greater information sharing between the private sector and the Federal Government. It preserves the privacy protections in the bill. When it was included in the House bill, both

Republicans and Democrats voted yes. I therefore ask my colleagues on both sides of the aisle to support this amendment.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

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

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

Mr. BURR. Mr. President, what is the order of business?

AMENDMENT NO. 2552, AS FURTHER MODIFIED

The PRESIDING OFFICER. Under the previous order, the question occurs on amendment No. 2552, as further modified, offered by the Senator from Delaware, Mr. COONS.

The Senator from California.

Mrs. FEINSTEIN. Mr. President, I wish to speak and urge a ''no'' vote on amendment No. 2552, known as the Coons amendment.

This amendment essentially adds another layer of review to the bill's current requirements. We worked this out in an earlier amendment with Senator CARPER. This amendment goes further, and it could prevent parts of the government from quickly learning about cyber threats at machine speed because it would require an additional privacy review for any information going through the DHS portal.

The Carper amendment that I spoke about was adopted as part of the managers' package, which made clear that the government should take automated steps to ensure that the real-time information sharing system can both protect privacy and allow for sharing at the speed necessary to stop cyber threats. Because the Coons amendment will slow down sharing via the DHS portal, I ask my colleagues to join me in voting no.

The PRESIDING OFFICER. The Senator from Delaware.

Mr. COONS. Mr. President, I rise today to urge my colleagues to support my amendment to make sure that this bill strikes the right balance between privacy and security.

I respect the very hard work of Senators BURR and FEINSTEIN and the constructive amendment that my senior Senator TOM CARPER added to the managers' amendment. I do believe this bill has made significant movement in the right direction. But I remain concerned, and my amendment's purpose is to require that DHS review all cyber threat indicators it receives and to remove personally identifying information by the most efficient means practicable. It would not necessarily—according to the amendment in the managers' package—be required that DHS scrub, unless multiple agency heads unanimously agree on the scrubbing process. My amendment's purpose is to simply ensure that these privacy scrubs—done at machine speed, done in a responsible way—protect citizen privacy and our security. I don't think we should be forced to choose between those two.

I urge my colleagues to support my amendment.

The PRESIDING OFFICER. The question occurs on agreeing to amendment No. 2552, as further modified.

Mr. BURR. I ask for the yeas and nays.

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The clerk will call the roll.

The legislative clerk called the roll.

Mr. CORNYN. The following Senators are necessarily absent: the Senator from Texas (Mr. CRUZ), the Senator from South Carolina (Mr. GRAHAM), the Senator from Kentucky (Mr. PAUL), the Senator from Florida (Mr. RUBIO), and the Senator from Louisiana (Mr. VITTER).

The PRESIDING OFFICER (Ms. AYOTTE). Are there any other Senators in the Chamber desiring to vote?

The result was announced—yeas 41, nays 54, as follows:

[Rollcall Vote No. 289 Leg.]

YEAS—41

| | | |
|---|---|---|
| Baldwin | Gillibrand | Peters |
| Bennet | Heinrich | Reed |
| Blumenthal | Heller | Reid |
| Booker | Hirono | Sanders |
| Boxer | Klobuchar | Schatz |
| Brown | Leahy | Schumer |
| Cantwell | Lee | Shaheen |
| Cardin | Markey | Stabenow |
| Coons | Menendez | Sullivan |
| Daines | Merkley | Tester |
| Durbin | Moran | Udall |
| Flake | Murkowski | Warren |
| Franken | Murphy | Wyden |
| Gardner | Murray | |

NAYS—54

| | | |
|---|---|---|
| Alexander | Enzi | McConnell |
| Ayotte | Ernst | Mikulski |
| Barrasso | Feinstein | Nelson |
| Blunt | Fischer | Perdue |
| Boozman | Grassley | Portman |
| Burr | Hatch | Risch |
| Capito | Heitkamp | Roberts |
| Carper | Hoeven | Rounds |
| Casey | Inhofe | Sasse |
| Cassidy | Isakson | Scott |
| Coats | Johnson | Sessions |
| Cochran | Kaine | Shelby |
| Collins | King | Thune |
| Corker | Kirk | Tillis |
| Cornyn | Lankford | Toomey |
| Cotton | Manchin | Warner |
| Crapo | McCain | Whitehouse |
| Donnelly | McCaskill | Wicker |

NOT VOTING—5

| | | |
|---|---|---|
| Cruz | Paul | Vitter |
| Graham | Rubio | |

The amendment (No. 2552), as further modified, was rejected.

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Madam President, I ask unanimous consent that the cloture motion on S. 754 be withdrawn; that prior to the vote on adoption of the Burr-Feinstein substitute amendment, the managers' amendment at the desk be agreed to; and that following adoption of the substitute, the bill be read a third time and the Senate vote on passage of the bill, as under the previous order. I further ask that notwithstanding adoption, the Flake amendment No. 2582 be modified with the technical change at the desk.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

The amendment (No. 2582), as further modified, is as follows:

At the end, add the following:

**SEC. 408. EFFECTIVE PERIOD.**

(a) IN GENERAL.—Except as provided in subsection (b), this Act and the amendments made by this Act shall be in effect during the 10-year period beginning on the date of the enactment of this Act.

(b) EXCEPTION.—With respect to any action authorized by this Act or information obtained pursuant to an action authorized by this Act, which occurred before the date on which the provisions referred to in subsection (a) cease to have effect, the provisions of this Act shall continue in effect.

AMENDMENT NO. 2581, AS MODIFIED

The PRESIDING OFFICER. Under the previous order, the question occurs on amendment No. 2581, as modified, offered by the Senator from Arkansas, Mr. COTTON.

The Senator from Arkansas.

Mr. COTTON. Madam President, I support this important bill, but I want to strengthen it.

Under the bill, a business receives liability protection by reporting threats to DHS or its regulatory agency, but many businesses, especially retailers like Target or Home Depot, don't have a regulator; thus, they must report to DHS. They have no choice. They must report to DHS even if they have longstanding ties to the FBI, as did Sony Pictures.

I contend that we should allow these businesses to choose between the DHS, FBI, and Secret Service. Fortunately, the White House appears to agree with my position. The National Security Council tweeted over the weekend: ''If you are a victim of a major cyber incident, a call to @FBI, @SecretService, or @DHSgov is a call to all.''

This amendment wouldn't undermine the single-point-of-reporting concept behind this bill because there is already an exception for the regulators, nor would it impair privacy rights because those rules apply to the FBI.

Finally, I would note that the House-passed version of this bill includes a nearly identical provision, and that got 307 votes.

Let's join together in a bipartisan fashion, adopt this amendment, and strengthen the bill.

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Madam President, we are almost at the end. This is the last amendment.

Unfortunately, I rise to ask my colleagues to vote against the amendment of not only my colleague but a member of the Intelligence Committee. This is a deal-killer. I will be very honest. This kills the deal. One of the thresholds that we had to reach was the balance to have one portal that the information goes through. This creates a new

portal. The White House is not in favor of it. Downtown is not in favor of it because they understand what it does.

We are this close right now to a voluntary information sharing bill. I can assure you that this is the first step. We have a ways to go. But if you want to stop it dead in its tracks, support this amendment. If, in fact, you want to get this across the goal line, then I would ask you to defeat the Cotton amendment and let us move to passage of this bill. Let us go to conference with the House.

I yield the floor.

The PRESIDING OFFICER. The question is on agreeing to the amendment, as modified.

Mr. BURR. I ask for the yeas and nays.

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The clerk will call the roll.

The senior assistant legislative clerk called the roll.

Mr. CORNYN. The following Senators are necessarily absent: the Senator from Texas (Mr. CRUZ), the Senator from South Carolina (Mr. GRAHAM), the Senator from Kentucky (Mr. PAUL), the Senator from Florida (Mr. RUBIO), and the Senator from Louisiana (Mr. VITTER).

The PRESIDING OFFICER. Are there any other Senators in the Chamber desiring to vote?

The result was announced—yeas 22, nays 73, as follows:

[Rollcall Vote No. 290 Leg.]

YEAS—22

| | | |
|---|---|---|
| Boozman | Kirk | Scott |
| Capito | Lankford | Sessions |
| Cornyn | McCain | Shelby |
| Cotton | McConnell | Thune |
| Fischer | Perdue | Toomey |
| Grassley | Portman | Whitehouse |
| Inhofe | Rounds | |
| Isakson | Sasse | |

NAYS—73

| | | |
|---|---|---|
| Alexander | Enzi | Moran |
| Ayotte | Ernst | Murkowski |
| Baldwin | Feinstein | Murphy |
| Barrasso | Flake | Murray |
| Bennet | Franken | Nelson |
| Blumenthal | Gardner | Peters |
| Blunt | Gillibrand | Reed |
| Booker | Hatch | Reid |
| Boxer | Heinrich | Risch |
| Brown | Heitkamp | Roberts |
| Burr | Heller | Sanders |
| Cantwell | Hirono | Schatz |
| Cardin | Hoeven | Schumer |
| Carper | Johnson | Shaheen |
| Casey | Kaine | Stabenow |
| Cassidy | King | Sullivan |
| Coats | Klobuchar | Tester |
| Cochran | Leahy | Tillis |
| Collins | Lee | Udall |
| Coons | Manchin | Warner |
| Corker | Markey | Warren |
| Crapo | McCaskill | Wicker |
| Daines | Menendez | Wyden |
| Donnelly | Merkley | |
| Durbin | Mikulski | |

NOT VOTING—5

| | | |
|---|---|---|
| Cruz | Paul | Vitter |
| Graham | Rubio | |

The amendment (No. 2581), as modified, was rejected.

Mr. COTTON. I yield back all time.

AMENDMENT NO. 2749 TO AMENDMENT NO. 2716

(Purpose: To improve the substitute amendment)

The PRESIDING OFFICER. Under the previous order, the managers' amendment, No. 2749, is agreed to.

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

VOTE ON AMENDMENT NO. 2716, AS AMENDED

The PRESIDING OFFICER. The question is on agreeing to the substitute amendment No. 2716, as amended.

The amendment (No. 2716), as amended, was agreed to.

The bill was ordered to be engrossed for a third reading and was read the third time.

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Madam President, I ask my colleagues for just the next 2 minutes to allow Senator FEINSTEIN and me to thank our colleagues for their help over the last several days as we have worked through the cyber bill.

I thank my vice chairman, who has been beside me all the way, and I thank Chairman JOHNSON and Ranking Member CARPER for the input they provided.

I want to say to committee staff who has worked night and day to get us to this point and to members of the committee who worked diligently for months to get this legislation enacted that I could not have done it without you.

Now the work begins as we go to conference.

I turn to the vice chairman.

Mrs. FEINSTEIN. I thank you very much.

Madam President, I just want to say a personal word to Chairman BURR, and maybe it is to everyone in this body. One of the things I have learned from two prior cyber bills is that if you really want to get a bill done, it has to be bipartisan, particularly a bill that is technical, difficult, and hard to put together, and a bill where often there are two sides. I thank you for recognizing this. We stood shoulder to shoulder and the right things happened, and now we can go to conference.

I also want to say that we did everything in this bill we possibly could to satisfy what were legitimate privacy concerns. The managers' package had 14 such amendments, and before that our staffs sat down with a number of proposals from Senators and went over literally dozens of additional amendments. So we took what we could.

When the chairman talks about the balance, what he means is that this is the first time the chamber of commerce has supported a bipartisan bill. This is the first time we had virtually all the big employers—banks and retailers and other companies—supporting a bipartisan bill because today everybody understands what the problem of cybersecurity is much greater. So we stood shoulder to shoulder, and you all responded, and I am very grateful.

There is still a lot of work to be done, but, Mr. Chairman, you and your staff have been terrific. I would like to single a couple of them out, if I might, in particular, Chris Joyner, Michael Geffroy, Jack Livingston, Janet Fisher, John Matchison, and Walter Weiss.

I also want to thank TOM CARPER, who has been working to get this bill passed as much as anyone. He wrote one of the key changes in the managers' package to improve privacy as information moves through the DHS portal. He was supported by his chairman, Senator JOHNSON. He has been a close partner throughout the process, and I thank him.

I also thank Gabbie Batkin, Matt Grote, and the other members of Senator CARPER's staff.

We had incredible support from our committee. It is a committee of 15—8 Republicans and 7 Democrats. I thank Senator COLLINS, who was particularly concerned about the critical infrastructure of this country, as well as Senators MIKULSKI, WHITEHOUSE, KING, WARNER, HEINRICH, BLUNT, NELSON, and COATS. I know they will help us push this bill forward as we go to conference with the House.

I greatly appreciate the supporters of this bill outside the Senate, to include the U.S. chamber of commerce and the associations that have endorsed this bill, tech companies like IBM and Oracle, Secretary Jeh Johnson at the Department of Homeland Security, and NSA Directors Keith Alexander and MIKE ROGERS, and Lisa Monaco and Michael Daniel at the White House.

On my staff, I would like to thank David Grannis, our staff director on the minority side. David has been there for these previous cyber bills, and it has proven to be a very difficult issue. David, you are a 10.

I also thank Josh Alexander. Josh has been our lead drafter and negotiator and knows these cyber issues better than anyone. He has been tireless on reaching agreement after agreement on this bill, and is, as much as anybody, responsible for today's vote.

I would also like to thank my former cyber staffer Andy Grotto, as well as Mike Buchwald, Brett Freedman, Nate Adler, and Nick Basciano. Thank you all so very much.

Finally, I very much appreciate the work done by Ayesha Khanna in the Democratic leader's office and Jeffrey Ratner at the White House.

We have the administration behind the bill, we have the Department of Homeland Security behind the bill, and we have the editorial pages of the Washington Post and the Wall Street Journal, as well as the chamber of commerce, and most of the businesses of America.

So, Mr. Chairman, you did a great job, and thank you from the bottom of my heart.

The PRESIDING OFFICER. The majority leader.

Mr. MCCONNELL. Madam President, I just want to add my words of congratulation to Chairman BURR and Ranking Member FEINSTEIN. This is a

very complicated issue, as we all know. It has been around multiple Congresses, and it took their leadership and coordination and cooperation first to produce a 14-to-1 vote in the committee and then this extraordinary success we have had out here on the floor. I know all of us are extremely proud of the great work you have done.

Congratulations. We deeply appreciate the contribution you have made to our country.

The PRESIDING OFFICER. The bill having been read the third time, the question is, Shall it pass?

Mr. TILLIS. I ask for the yeas and nays.

The PRESIDING OFFICER. Is there a sufficient second?

There is a sufficient second.

The clerk will call the roll.

The bill clerk called the roll.

Mr. CORNYN. The following Senators are necessarily absent: the Senator from Texas (Mr. CRUZ), the Senator from South Carolina (Mr. GRAHAM), the Senator from Kentucky (Mr. PAUL), the Senator from Florida (Mr. RUBIO), and the Senator from Louisiana (Mr. VITTER).

The PRESIDING OFFICER. Are there any other Senators in the Chamber desiring to vote?

The result was announced—yeas 74, nays 21, as follows:

[Rollcall Vote No. 291 Leg.]

YEAS—74

| | | |
|---|---|---|
| Alexander | Fischer | Murphy |
| Ayotte | Flake | Murray |
| Barrasso | Gardner | Nelson |
| Bennet | Gillibrand | Perdue |
| Blumenthal | Grassley | Peters |
| Blunt | Hatch | Portman |
| Boozman | Heinrich | Reed |
| Boxer | Heitkamp | Reid |
| Burr | Hirono | Roberts |
| Cantwell | Hoeven | Rounds |
| Capito | Inhofe | Sasse |
| Carper | Isakson | Schatz |
| Casey | Johnson | Schumer |
| Cassidy | Kaine | Scott |
| Coats | King | Sessions |
| Cochran | Kirk | Shaheen |
| Collins | Klobuchar | Shelby |
| Corker | Lankford | Stabenow |
| Cornyn | Manchin | Thune |
| Cotton | McCain | Tillis |
| Donnelly | McCaskill | Toomey |
| Durbin | McConnell | Warner |
| Enzi | Mikulski | Whitehouse |
| Ernst | Moran | Wicker |
| Feinstein | Murkowski | |

NAYS—21

| | | |
|---|---|---|
| Baldwin | Franken | Risch |
| Booker | Heller | Sanders |
| Brown | Leahy | Sullivan |
| Cardin | Lee | Tester |
| Coons | Markey | Udall |
| Crapo | Menendez | Warren |
| Daines | Merkley | Wyden |

NOT VOTING—5

| | | |
|---|---|---|
| Cruz | Paul | Vitter |
| Graham | Rubio | |

The bill (S. 754), as amended, was passed, as follows:

S. 754

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

**SECTION 1. TABLE OF CONTENTS.**

The table of contents of this Act is as follows:



## TITLE I—CYBERSECURITY INFORMATION SHARING

**SEC. 101. SHORT TITLE.**

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

**SEC. 102. DEFINITIONS.**

In this title:

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

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

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

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

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

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

(A) The Department of Commerce.

(B) The Department of Defense.

(C) The Department of Energy.

(D) The Department of Homeland Security.

(E) The Department of Justice.

(F) The Department of the Treasury.

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

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

(5) CYBERSECURITY THREAT.—

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

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

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

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

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

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

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

(E) malicious cyber command and control;

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

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

(H) any combination thereof.

(7) DEFENSIVE MEASURE.—

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

(B) EXCLUSION.—The term ''defensive measure'' does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or data on an information system not belonging to—

(i) the private entity operating the measure; or

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

(8) ENTITY.—

(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term ''entity'' means any private entity, non-Federal government agency or department, or State,

tribal, or local government (including a political subdivision, department, or component thereof).

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

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

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

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

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

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

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

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

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

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

(15) PRIVATE ENTITY.—

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

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

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

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

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

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

**SEC. 103. SHARING OF INFORMATION BY THE FEDERAL GOVERNMENT.**

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

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

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

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

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

(5) the periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analysis of cyber threat indicators and information in possession of the Federal Government, with attention to accessibility and implementation challenges faced by small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 632)).

(b) DEVELOPMENT OF PROCEDURES.—

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

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

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

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

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

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

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

(ii) to implement and utilize a technical capability configured to remove any personal information or information that identifies a specific person not directly related to a cybersecurity threat; and

(F) include procedures for notifying, in a timely manner, any United States person whose personal information is known or determined to have been shared by a Federal entity in violation of this Act.

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

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

**SEC. 104. AUTHORIZATIONS FOR PREVENTING, DETECTING, ANALYZING, AND MITIGATING CYBERSECURITY THREATS.**

(a) AUTHORIZATION FOR MONITORING.—

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

(A) an information system of such private entity;

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

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

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

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

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

(B) to limit otherwise lawful activity.

(b) AUTHORIZATION FOR OPERATION OF DEFENSIVE MEASURES.—

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

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

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

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

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

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

(B) to limit otherwise lawful activity.

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

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

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

measure by the sharing entity or Federal entity.

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

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

(B) to limit otherwise lawful activity.

(d) PROTECTION AND USE OF INFORMATION.—

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

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

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

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

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

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

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

(I) an information system of the entity; or

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

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

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

(II) an otherwise applicable provision of law.

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

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

(A) LAW ENFORCEMENT USE.—

(i) PRIOR WRITTEN CONSENT.—Except as provided in clause (ii), a cyber threat indicator shared with a State, tribal, or local government under this section may, with the prior written consent of the entity sharing such indicator, be used by a State, tribal, or local government for the purpose of preventing, investigating, or prosecuting any of the offenses described in section 105(d)(5)(A)(vi).

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

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

(i) deemed voluntarily shared information; and

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

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

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

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

(e) ANTITRUST EXEMPTION.—

(1) IN GENERAL.—Except as provided in section 108(e), it shall not be considered a violation of any provision of antitrust laws for 2 or more private entities to exchange or provide a cyber threat indicator, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat, for cybersecurity purposes under this title.

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

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

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

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

**SEC. 105. SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH THE FEDERAL GOVERNMENT.**

(a) REQUIREMENT FOR POLICIES AND PROCEDURES.—

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

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

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

(A) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 104(c) through the real-time process described in subsection (c) of this section—

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

(ii) are only subject to a delay, modification, or other action due to controls established for such real-time process that could impede real-time receipt by all of the appropriate Federal entities when the delay, modification, or other action is due to controls—

(I) agreed upon unanimously by all of the heads of the appropriate Federal entities;

(II) carried out before any of the appropriate Federal entities retains or uses the cyber threat indicators or defensive measures; and

(III) uniformly applied such that each of the appropriate Federal entities is subject to the same delay, modification, or other action; and

(iii) may be provided to other Federal entities;

(B) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 104 in a manner other than the real time process described in subsection (c) of this section—

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

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

(iii) may be provided to other Federal entities;

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

(D) ensure there are—

(i) audit capabilities; and

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

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

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

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

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

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

(iii) Such other matters as the Attorney General and the Secretary of Homeland Security consider appropriate for entities sharing cyber threat indicators with Federal entities under this title.

(b) PRIVACY AND CIVIL LIBERTIES.—

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

(2) FINAL GUIDELINES.—

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

(B) PERIODIC REVIEW.—The Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers and private entities described in subparagraph (A), periodically, but not less frequently than once every two years, review the guidelines promulgated under subparagraph (A).

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

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

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

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

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

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

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

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

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

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

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

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

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

(i) consistent with section 104, communications between a Federal entity and a private entity regarding a previously shared cyber threat indicator to describe the relevant cybersecurity threat or develop a defensive measure based on such cyber threat indicator; and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(5) REPORT ON DEVELOPMENT AND IMPLEMENTATION.—

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

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

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

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

(2) PROPRIETARY INFORMATION.—Consistent with section 104(c)(2), a cyber threat indicator or defensive measure provided by an entity to the Federal Government under this title shall be considered the commercial, financial, and proprietary information of such entity when so designated by the originating entity or a third party acting in accordance with the written authorization of the originating entity.

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

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

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

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

(5) DISCLOSURE, RETENTION, AND USE.—

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

(i) a cybersecurity purpose;

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

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

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

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

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

(I) sections 1028 through 1030 of title 18, United States Code (relating to fraud and identity theft);

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

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

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

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

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

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

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

(D) FEDERAL REGULATORY AUTHORITY.—

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

(ii) EXCEPTIONS.—

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

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

**SEC. 106. PROTECTION FROM LIABILITY.**

(a) MONITORING OF INFORMATION SYSTEMS.—No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of information systems and information under section 104(a) that is conducted in accordance with this title.

(b) SHARING OR RECEIPT OF CYBER THREAT INDICATORS.—No cause of action shall lie or be maintained in any court against any entity, and such action shall be promptly dismissed, for the sharing or receipt of cyber threat indicators or defensive measures under section 104(c) if—

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

(2) in a case in which a cyber threat indicator or defensive measure is shared with the Federal Government, the cyber threat indicator or defensive measure is shared in a manner that is consistent with section 105(c)(1)(B) and the sharing or receipt, as the case may be, occurs after the earlier of—

(A) the date on which the interim policies and procedures are submitted to Congress under section 105(a)(1) and guidelines are submitted to Congress under section 105(b)(1); or

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

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

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

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

**SEC. 107. OVERSIGHT OF GOVERNMENT ACTIVITIES.**

(a) BIENNIAL REPORT ON IMPLEMENTATION.—

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

(A) in the case of the first report submitted under this paragraph, the most recent 1-year period; and

(B) in the case of any subsequent report submitted under this paragraph, the most recent 2-year period.

(2) CONTENTS.—Each report submitted under paragraph (1) shall include, for the period covered by the report, the following:

(A) An assessment of the sufficiency of the policies, procedures, and guidelines required by section 105 in ensuring that cyber threat indicators are shared effectively and responsibly within the Federal Government.

(B) An evaluation of the effectiveness of real-time information sharing through the capability and process developed under section 105(c), including any impediments to such real-time sharing.

(C) An assessment of the sufficiency of the procedures developed under section 103 in ensuring that cyber threat indicators in the possession of the Federal Government are shared in a timely and adequate manner with appropriate entities, or, if appropriate, are made publicly available.

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

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

(i) The number of cyber threat indicators received through the capability and process developed under section 105(c).

(ii) The number of times that information shared under this title was used by a Federal entity to prosecute an offense consistent with section 105(d)(5)(A).

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

(iv) A quantitative and qualitative assessment of the effect of the sharing of such cyber threat indicators with the Federal Government on privacy and civil liberties of specific persons, including the number of notices that were issued with respect to a failure to remove personal information or information that identified a specific person not directly related to a cybersecurity threat in accordance with the procedures required by section 105(b)(3)(D).

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

(F) A review of actions taken by the Federal Government based on cyber threat indicators shared with the Federal Government under this title, including the appropriateness of any subsequent use or dissemination of such cyber threat indicators by a Federal entity under section 105.

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

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

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

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

(b) REPORTS ON PRIVACY AND CIVIL LIBERTIES.—

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

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

(B) an assessment of the sufficiency of the policies, procedures, and guidelines established pursuant to section 105 in addressing concerns relating to privacy and civil liberties.

(2) BIENNIAL REPORT OF INSPECTORS GENERAL.—

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

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

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

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

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

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

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

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

**SEC. 108. CONSTRUCTION AND PREEMPTION.**

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

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

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

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

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

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

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

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

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

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

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

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

(2) to prohibit a new information sharing relationship;

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

(4) to require the use of the capability and process within the Department of Homeland Security developed under section 105(c).

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

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

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

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

(1) to require an entity to provide information to a Federal entity or another entity;

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

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

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

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

(k) FEDERAL PREEMPTION.—

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

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

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

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

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

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

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

**SEC. 109. REPORT ON CYBERSECURITY THREATS.**

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

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

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

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

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

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

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

(c) ADDITIONAL REPORT.—At the time the report required by subsection (a) is submitted, the Director of National Intelligence shall submit to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives a report containing the information required by subsection (b)(2).

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

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

**SEC. 110. CONFORMING AMENDMENT.**

Section 941(c)(3) of the National Defense Authorization Act for Fiscal Year 2013 (Public Law 112–239; 10 U.S.C. 2224 note) is amended by inserting at the end the following: ''The Secretary may share such information with other Federal entities if such information consists of cyber threat indicators and defensive measures and such information is shared consistent with the policies and procedures promulgated by the Attorney General and the Secretary of Homeland Security under section 105 of the Cybersecurity Information Sharing Act of 2015.''.

## TITLE II—FEDERAL CYBERSECURITY ENHANCEMENT

**SEC. 201. SHORT TITLE.**

This title may be cited as the ''Federal Cybersecurity Enhancement Act of 2015''.

**SEC. 202. DEFINITIONS.**

In this title—

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

(2) the term ''agency information system'' has the meaning given the term in section 228 of the Homeland Security Act of 2002, as added by section 203(a);

(3) the term ''appropriate congressional committees'' means—

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

(B) the Committee on Homeland Security of the House of Representatives;

(4) the terms ''cybersecurity risk'' and ''information system'' have the meanings given those terms in section 227 of the Homeland Security Act of 2002, as so redesignated by section 203(a);

(5) the term ''Director'' means the Director of the Office of Management and Budget;

(6) the term ''intelligence community'' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4));

(7) the term ''national security system'' has the meaning given the term in section 11103 of title 40, United States Code; and

(8) the term ''Secretary'' means the Secretary of Homeland Security.

**SEC. 203. IMPROVED FEDERAL NETWORK SECURITY.**

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended—

(1) by redesignating section 228 as section 229;

(2) by redesignating section 227 as subsection (c) of section 228, as added by paragraph (4), and adjusting the margins accordingly;

(3) by redesignating the second section designated as section 226 (relating to the national cybersecurity and communications integration center) as section 227;

(4) by inserting after section 227, as so redesignated, the following:

**''SEC. 228. CYBERSECURITY PLANS.**

''(a) DEFINITIONS.—In this section—

''(1) the term 'agency information system' means an information system used or operated by an agency or by another entity on behalf of an agency;

''(2) the terms 'cybersecurity risk' and 'information system' have the meanings given those terms in section 227;

''(3) the term 'intelligence community' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)); and

''(4) the term 'national security system' has the meaning given the term in section 11103 of title 40, United States Code.

''(b) INTRUSION ASSESSMENT PLAN.—

''(1) REQUIREMENT.—The Secretary, in coordination with the Director of the Office of Management and Budget, shall develop and implement an intrusion assessment plan to identify and remove intruders in agency information systems.

''(2) EXCEPTION.—The intrusion assessment plan required under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.'';

(5) in section 228(c), as so redesignated, by striking ''section 226'' and inserting ''section 227''; and

(6) by inserting after section 229, as so redesignated, the following:

**''SEC. 230. FEDERAL INTRUSION DETECTION AND PREVENTION SYSTEM.**

''(a) DEFINITIONS.—In this section—

''(1) the term 'agency' has the meaning given that term in section 3502 of title 44, United States Code;

''(2) the term 'agency information' means information collected or maintained by or on behalf of an agency;

''(3) the term 'agency information system' has the meaning given the term in section 228; and

''(4) the terms 'cybersecurity risk' and 'information system' have the meanings given those terms in section 227.

''(b) REQUIREMENT.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of this section, the Secretary shall deploy, operate, and maintain, to make available for use by any agency, with or without reimbursement—

''(A) a capability to detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system; and

''(B) a capability to prevent network traffic associated with such cybersecurity risks from transiting or traveling to or from an agency information system or modify such network traffic to remove the cybersecurity risk.

''(2) REGULAR IMPROVEMENT.—The Secretary shall regularly deploy new technologies and modify existing technologies to the intrusion detection and prevention capabilities described in paragraph (1) as appropriate to improve the intrusion detection and prevention capabilities.

''(c) ACTIVITIES.—In carrying out subsection (b), the Secretary—

''(1) may access, and the head of an agency may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information transiting or traveling to or from an agency information system, regardless of the location from which the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or prevent the head of an agency from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);

''(2) may enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy and operate technologies in accordance with subsection (b);

''(3) may retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect information and information systems from cybersecurity risks;

''(4) shall regularly assess through operational test and evaluation in real world or simulated environments available advanced protective technologies to improve detection and prevention capabilities, including commercial and non-commercial technologies and detection technologies beyond signature-based detection, and utilize such technologies when appropriate;

''(5) shall establish a pilot to acquire, test, and deploy, as rapidly as possible, technologies described in paragraph (4);

''(6) shall periodically update the privacy impact assessment required under section 208(b) of the E-Government Act of 2002 (44 U.S.C. 3501 note); and

''(7) shall ensure that—

''(A) activities carried out under this section are reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

''(B) information accessed by the Secretary will be retained no longer than reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

''(C) notice has been provided to users of an agency information system concerning access to communications of users of the agency information system for the purpose of protecting agency information and the agency information system; and

''(D) the activities are implemented pursuant to policies and procedures governing the operation of the intrusion detection and prevention capabilities.

''(d) PRIVATE ENTITIES.—

''(1) CONDITIONS.—A private entity described in subsection (c)(2) may not—

''(A) disclose any network traffic transiting or traveling to or from an agency information system to any entity without the consent of the Department or the agency that disclosed the information under subsection (c)(1); or

''(B) use any network traffic transiting or traveling to or from an agency information system to which the private entity gains access in accordance with this section for any purpose other than to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to subsection (c)(2) or as part of another contract with the Secretary.

''(2) LIMITATION ON LIABILITY.—No cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to subsection (c)(2).

''(3) RULE OF CONSTRUCTION.—Nothing in paragraph (2) shall be construed to authorize an Internet service provider to break a user agreement with a customer without the consent of the customer.

''(e) ATTORNEY GENERAL REVIEW.—Not later than 1 year after the date of enactment of this section, the Attorney General shall review the policies and guidelines for the program carried out under this section to ensure that the policies and guidelines are consistent with applicable law governing the acquisition, interception, retention, use, and disclosure of communications.''.

(b) PRIORITIZING ADVANCED SECURITY TOOLS.—The Director and the Secretary, in consultation with appropriate agencies, shall—

(1) review and update governmentwide policies and programs to ensure appropriate prioritization and use of network security monitoring tools within agency networks; and

(2) brief appropriate congressional committees on such prioritization and use.

(c) AGENCY RESPONSIBILITIES.—

(1) IN GENERAL.—Except as provided in paragraph (2)—

(A) not later than 1 year after the date of enactment of this Act or 2 months after the date on which the Secretary makes available the intrusion detection and prevention capabilities under section 230(b)(1) of the Homeland Security Act of 2002, as added by subsection (a), whichever is later, the head of each agency shall apply and continue to utilize the capabilities to all information traveling between an agency information system and any information system other than an agency information system; and

(B) not later than 6 months after the date on which the Secretary makes available improvements to the intrusion detection and prevention capabilities pursuant to section 230(b)(2) of the Homeland Security Act of 2002, as added by subsection (a), the head of each agency shall apply and continue to utilize the improved intrusion detection and prevention capabilities.

(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(3) DEFINITION.—In this subsection only, the term ''agency information system'' means an information system owned or operated by an agency.

(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to limit an agency from applying the intrusion detection and prevention capabilities under section 230(b)(1) of the Homeland Security Act of 2002, as added by subsection (a), at the discretion of the head of the agency or as provided in relevant policies, directives, and guidelines.

(d) TABLE OF CONTENTS AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 note) is amended by striking the items relating to the first section designated as section 226, the second section designated as section 226 (relating to the national cybersecurity and communications integration center), section 227, and section 228 and inserting the following:

''Sec. 226. Cybersecurity recruitment and retention.

''Sec. 227. National cybersecurity and communications integration center.

**SEC. 204. ADVANCED INTERNAL DEFENSES.**

(a) ADVANCED NETWORK SECURITY TOOLS.—

(1) IN GENERAL.—The Secretary shall include in the Continuous Diagnostics and Mitigation Program advanced network security tools to improve visibility of network activity, including through the use of commercial and free or open source tools, to detect and mitigate intrusions and anomalous activity.

(2) DEVELOPMENT OF PLAN.—The Director shall develop and implement a plan to ensure that each agency utilizes advanced network security tools, including those described in paragraph (1), to detect and mitigate intrusions and anomalous activity.

(b) IMPROVED METRICS.—The Secretary, in collaboration with the Director, shall review and update the metrics used to measure security under section 3554 of title 44, United States Code, to include measures of intrusion and incident detection and response times.

(c) TRANSPARENCY AND ACCOUNTABILITY.—The Director, in consultation with the Secretary, shall increase transparency to the public on agency cybersecurity posture, including by increasing the number of metrics available on Federal Government performance websites and, to the greatest extent practicable, displaying metrics for department components, small agencies, and micro agencies.

(d) MAINTENANCE OF TECHNOLOGIES.—Section 3553(b)(6)(B) of title 44, United States Code, is amended by inserting '', operating, and maintaining'' after ''deploying''.

(e) EXCEPTION.—The requirements under this section shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

**SEC. 205. FEDERAL CYBERSECURITY REQUIREMENTS.**

(a) IMPLEMENTATION OF FEDERAL CYBERSECURITY STANDARDS.—Consistent with section 3553 of title 44, United States Code, the Secretary, in consultation with the Director, shall exercise the authority to issue binding operational directives to assist the Director in ensuring timely agency adoption of and compliance with policies and standards promulgated under section 11331 of title 40, United States Code, for securing agency information systems.

(b) CYBERSECURITY REQUIREMENTS AT AGENCIES.—

(1) IN GENERAL.—Consistent with policies, standards, guidelines, and directives on information security under subchapter II of chapter 35 of title 44, United States Code, and the standards and guidelines promulgated under section 11331 of title 40, United States Code, and except as provided in paragraph (2), not later than 1 year after the date of the enactment of this Act, the head of each agency shall—

(A) identify sensitive and mission critical data stored by the agency consistent with the inventory required under the first subsection (c) (relating to the inventory of major information systems) and the second subsection (c) (relating to the inventory of information systems) of section 3505 of title 44, United States Code;

(B) assess access controls to the data described in subparagraph (A), the need for readily accessible storage of the data, and individuals' need to access the data;

(C) encrypt or otherwise render indecipherable to unauthorized users the data described in subparagraph (A) that is stored on or transiting agency information systems;

(D) implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication, as developed by the Administrator of General Services in collaboration with the Secretary; and

(E) implement identity management consistent with section 504 of the Cybersecurity Enhancement Act of 2014 (Public Law 113–274; 15 U.S.C. 7464), including multi-factor authentication, for—

(i) remote access to an agency information system; and

(ii) each user account with elevated privileges on an agency information system.

(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to an agency information system for which—

(A) the head of the agency has personally certified to the Director with particularity that—

(i) operational requirements articulated in the certification and related to the agency information system would make it excessively burdensome to implement the cybersecurity requirement;

(ii) the cybersecurity requirement is not necessary to secure the agency information system or agency information stored on or transiting it; and

(iii) the agency has taken all necessary steps to secure the agency information system and agency information stored on or transiting it; and

(B) the head of the agency or the designee of the head of the agency has submitted the certification described in subparagraph (A) to the appropriate congressional committees and the agency's authorizing committees.

(3) CONSTRUCTION.—Nothing in this section shall be construed to alter the authority of the Secretary, the Director, or the Director of the National Institute of Standards and Technology in implementing subchapter II of chapter 35 of title 44, United States Code. Nothing in this section shall be construed to affect the National Institute of Standards and Technology standards process or the requirement under section 3553(a)(4) of such title or to discourage continued improvements and advancements in the technology, standards, policies, and guidelines used to promote Federal information security.

(c) EXCEPTION.—The requirements under this section shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

**SEC. 206. ASSESSMENT; REPORTS.**

(a) DEFINITIONS.—In this section—

(1) the term ''intrusion assessments'' means actions taken under the intrusion assessment plan to identify and remove intruders in agency information systems;

(2) the term ''intrusion assessment plan'' means the plan required under section 228(b)(1) of the Homeland Security Act of 2002, as added by section 203(a) of this Act; and

(3) the term ''intrusion detection and prevention capabilities'' means the capabilities required under section 230(b) of the Homeland Security Act of 2002, as added by section 203(a) of this Act.

(b) THIRD PARTY ASSESSMENT.—Not later than 3 years after the date of enactment of this Act, the Government Accountability Office shall conduct a study and publish a report on the effectiveness of the approach and strategy of the Federal Government to securing agency information systems, including the intrusion detection and prevention capabilities and the intrusion assessment plan.

(c) REPORTS TO CONGRESS.—

(1) INTRUSION DETECTION AND PREVENTION CAPABILITIES.—

(A) SECRETARY OF HOMELAND SECURITY REPORT.—Not later than 6 months after the date of enactment of this Act, and annually thereafter, the Secretary shall submit to the appropriate congressional committees a report on the status of implementation of the intrusion detection and prevention capabilities, including—

(i) a description of privacy controls;

(ii) a description of the technologies and capabilities utilized to detect cybersecurity risks in network traffic, including the extent to which those technologies and capabilities include existing commercial and non-commercial technologies;

(iii) a description of the technologies and capabilities utilized to prevent network traffic associated with cybersecurity risks from transiting or traveling to or from agency information systems, including the extent to which those technologies and capabilities include existing commercial and non-commercial technologies;

(iv) a list of the types of indicators or other identifiers or techniques used to detect cybersecurity risks in network traffic transiting or traveling to or from agency information systems on each iteration of the intrusion detection and prevention capabilities and the number of each such type of indicator, identifier, and technique;

(v) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from agency information systems and the number of times the intrusion detection and prevention capabilities blocked network traffic associated with cybersecurity risk; and

(vi) a description of the pilot established under section 230(c)(5) of the Homeland Security Act of 2002, as added by section 203(a) of this Act, including the number of new technologies tested and the number of participating agencies.

(B) OMB REPORT.—Not later than 18 months after the date of enactment of this Act, and annually thereafter, the Director shall submit to Congress, as part of the report required under section 3553(c) of title 44, United States Code, an analysis of agency application of the intrusion detection and prevention capabilities, including—

(i) a list of each agency and the degree to which each agency has applied the intrusion detection and prevention capabilities to an agency information system; and

(ii) a list by agency of—

(I) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such cybersecurity risks; and

(II) the number of instances in which the intrusion detection and prevention capabilities prevented network traffic associated with a cybersecurity risk from transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such agency information systems.

(2) OMB REPORT ON DEVELOPMENT AND IMPLEMENTATION OF INTRUSION ASSESSMENT PLAN, ADVANCED INTERNAL DEFENSES, AND FEDERAL CYBERSECURITY BEST PRACTICES.—The Director shall—

(A) not later than 6 months after the date of enactment of this Act, and 30 days after any update thereto, submit the intrusion assessment plan to the appropriate congressional committees;

(B) not later than 1 year after the date of enactment of this Act, and annually thereafter, submit to Congress, as part of the report required under section 3553(c) of title 44, United States Code—

(i) a description of the implementation of the intrusion assessment plan;

(ii) the findings of the intrusion assessments conducted pursuant to the intrusion assessment plan;

(iii) advanced network security tools included in the Continuous Diagnostics and Mitigation Program pursuant to section 204(a)(1);

(iv) the results of the assessment of the Secretary of best practices for Federal cybersecurity pursuant to section 205(a); and

(v) a list by agency of compliance with the requirements of section 205(b); and

(C) not later than 1 year after the date of enactment of this Act, submit to the appropriate congressional committees—

(i) a copy of the plan developed pursuant to section 204(a)(2); and

(ii) the improved metrics developed pursuant to section 204(b).

**SEC. 207. TERMINATION.**

(a) IN GENERAL.—The authority provided under section 230 of the Homeland Security Act of 2002, as added by section 203(a) of this Act, and the reporting requirements under section 206(c) shall terminate on the date that is 7 years after the date of enactment of this Act.

(b) RULE OF CONSTRUCTION.—Nothing in subsection (a) shall be construed to affect the limitation of liability of a private entity for assistance provided to the Secretary under section 230(d)(2) of the Homeland Security Act of 2002, as added by section 203(a) of this Act, if such assistance was rendered before the termination date under subsection (a) or otherwise during a period in which the assistance was authorized.

**SEC. 208. IDENTIFICATION OF INFORMATION SYSTEMS RELATING TO NATIONAL SECURITY.**

(a) IN GENERAL.—Except as provided in subsection (c), not later than 180 days after the date of enactment of this Act—

(1) the Director of National Intelligence and the Director of the Office of Management and Budget, in coordination with the heads of other agencies, shall—

(A) identify all unclassified information systems that provide access to information that may provide an adversary with the ability to derive information that would otherwise be considered classified;

(B) assess the risks that would result from the breach of each unclassified information system identified in subparagraph (A); and

(C) assess the cost and impact on the mission carried out by each agency that owns an unclassified information system identified in subparagraph (A) if the system were to be subsequently designated as a national security system; and

(2) the Director of National Intelligence and the Director of the Office of Management and Budget shall submit to the appropriate congressional committees, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives a report that includes the findings under paragraph (1).

(b) FORM.—The report submitted under subsection (a)(2) shall be in unclassified form, and shall include a classified annex.

(c) EXCEPTION.—The requirements under subsection (a)(1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to designate an information system as a national security system.

**SEC. 209. DIRECTION TO AGENCIES.**

(a) IN GENERAL.—Section 3553 of title 44, United States Code, is amended by adding at the end the following:

''(h) DIRECTION TO AGENCIES.—

''(1) AUTHORITY.—

''(A) IN GENERAL.—Subject to subparagraph (B), in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, the Secretary may issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat.

''(B) EXCEPTION.—The authorities of the Secretary under this subsection shall not apply to a system described subsection (d) or to a system described in paragraph (2) or (3) of subsection (e).

''(2) PROCEDURES FOR USE OF AUTHORITY.—The Secretary shall—

''(A) in coordination with the Director, establish procedures governing the circumstances under which a directive may be issued under this subsection, which shall include—

''(i) thresholds and other criteria;

''(ii) privacy and civil liberties protections; and

''(iii) providing notice to potentially affected third parties;

''(B) specify the reasons for the required action and the duration of the directive;

''(C) minimize the impact of a directive under this subsection by—

''(i) adopting the least intrusive means possible under the circumstances to secure the agency information systems; and

''(ii) limiting directives to the shortest period practicable;

''(D) notify the Director and the head of any affected agency immediately upon the issuance of a directive under this subsection;

''(E) consult with the Director of the National Institute of Standards and Technology regarding any directive under this subsection that implements standards and guidelines developed by the National Institute of Standards and Technology;

''(F) ensure that directives issued under this subsection do not conflict with the standards and guidelines issued under section 11331 of title 40;

''(G) consider any applicable standards or guidelines developed by the National Institute of Standards and issued by the Secretary of Commerce under section 11331 of title 40; and

''(H) not later than February 1 of each year, submit to the appropriate congressional committees a report regarding the specific actions the Secretary has taken pursuant to paragraph (1)(A).

''(3) IMMINENT THREATS.—

''(A) IN GENERAL.—Notwithstanding section 3554, the Secretary may authorize the intrusion detection and prevention capabilities under section 230(b)(1) of the Homeland Security Act of 2002 for the purpose of ensuring the security of agency information systems, if—

''(i) the Secretary determines there is an imminent threat to agency information systems;

''(ii) the Secretary determines a directive under subsection (b)(2)(C) or paragraph (1)(A) is not reasonably likely to result in a timely response to the threat;

''(iii) the Secretary determines the risk posed by the imminent threat outweighs any adverse consequences reasonably expected to result from the use of protective capabilities under the control of the Secretary;

''(iv) the Secretary provides prior notice to the Director, and the head and chief information officer (or equivalent official) of each agency to which specific actions will be taken pursuant to subparagraph (A), and notifies the appropriate congressional committees and authorizing committees of each such agencies within seven days of taking an action under this subsection of—

''(I) any action taken under this subsection; and

''(II) the reasons for and duration and nature of the action;

''(v) the action of the Secretary is consistent with applicable law; and

''(vi) the Secretary authorizes the use of protective capabilities in accordance with the advance procedures established under subparagraph (C).

''(B) LIMITATION ON DELEGATION.—The authority under this subsection may not be delegated by the Secretary.

''(C) ADVANCE PROCEDURES.—The Secretary shall, in coordination with the Director, and in consultation with the heads of Federal agencies, establish procedures governing the circumstances under which the Secretary may authorize the use of protective capabilities subparagraph (A). The Secretary shall submit the procedures to Congress.

''(4) LIMITATION.—The Secretary may direct or authorize lawful action or protective capability under this subsection only to—

''(A) protect agency information from unauthorized access, use, disclosure, disruption, modification, or destruction; or

''(B) require the remediation of or protect against identified information security risks with respect to—

''(i) information collected or maintained by or on behalf of an agency; or

''(ii) that portion of an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

''(i) ANNUAL REPORT TO CONGRESS.—Not later than February 1 of each year, the Director shall submit to the appropriate congressional committees a report regarding the specific actions the Director has taken pursuant to subsection (a)(5), including any actions taken pursuant to section 11303(b)(5) of title 40.

''(j) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term 'appropriate congressional committees' means—

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

''(2) the Committee on Appropriations, the Committee on Homeland Security, the Committee on Oversight and Government Reform, and the Committee on Science, Space, and Technology of the House of Representatives.''.

(b) CONFORMING AMENDMENT.—Section 3554(a)(1)(B) of title 44, United States Code, is amended—

(1) in clause (iii), by striking ''and'' at the end; and

(2) by adding at the end the following:

''(v) emergency directives issued by the Secretary under section 3553(h); and''.

## TITLE III—FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT

**SEC. 301. SHORT TITLE.**

This title may be cited as the ''Federal Cybersecurity Workforce Assessment Act of 2015''.

**SEC. 302. DEFINITIONS.**

In this title:

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

(A) the Committee on Armed Services of the Senate;

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

(C) the Select Committee on Intelligence of the Senate;

(D) the Committee on Commerce, Science, and Transportation of the Senate;

(E) the Committee on Armed Services in the House of Representatives;

(F) the Committee on Homeland Security of the House of Representatives;

(G) the Committee on Oversight and Government Reform of the House of Representatives; and

(H) the Permanent Select Committee on Intelligence of the House of Representatives.

(2) DIRECTOR.—The term ''Director'' means the Director of the Office of Personnel Management.

(3) ROLES.—The term ''roles'' has the meaning given the term in the National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework.

**SEC. 303. NATIONAL CYBERSECURITY WORKFORCE MEASUREMENT INITIATIVE.**

(a) IN GENERAL.—The head of each Federal agency shall—

(1) identify all positions within the agency that require the performance of cybersecurity or other cyber-related functions; and

(2) assign the corresponding employment code, which shall be added to the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework, in accordance with subsection (b).

(b) EMPLOYMENT CODES.—

(1) PROCEDURES.—

(A) CODING STRUCTURE.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Commerce, acting through the National Institute of Standards and Technology, shall update the National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework to include a corresponding coding structure.

(B) IDENTIFICATION OF CIVILIAN CYBER PERSONNEL.—Not later than 9 months after the date of enactment of this Act, the Director, in coordination with the Director of the National Institute of Standards and Technology and the Director of National Intelligence, shall establish procedures to implement the National Initiative for Cybersecurity Education's coding structure to identify all Federal civilian positions that require the performance of information technology, cybersecurity, or other cyber-related functions.

(C) IDENTIFICATION OF NONCIVILIAN CYBER PERSONNEL.—Not later than 18 months after the date of enactment of this Act, the Secretary of Defense shall establish procedures to implement the National Initiative for Cybersecurity Education's coding structure to identify all Federal noncivilian positions that require the performance of information technology, cybersecurity, or other cyber-related functions.

(D) BASELINE ASSESSMENT OF EXISTING CYBERSECURITY WORKFORCE.—Not later than 3 months after the date on which the procedures are developed under subparagraphs (B) and (C), respectively, the head of each Federal agency shall submit to the appropriate congressional committees of jurisdiction a report that identifies—

(i) the percentage of personnel with information technology, cybersecurity, or other cyber-related job functions who currently hold the appropriate industry-recognized certifications as identified in the National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework;

(ii) the level of preparedness of other civilian and noncivilian cyber personnel without existing credentials to take certification exams; and

(iii) a strategy for mitigating any gaps identified in clause (i) or (ii) with the appropriate training and certification for existing personnel.

(E) PROCEDURES FOR ASSIGNING CODES.—Not later than 3 months after the date on which the procedures are developed under subparagraphs (B) and (C), respectively, the head of each Federal agency shall establish procedures—

(i) to identify all encumbered and vacant positions with information technology, cybersecurity, or other cyber-related functions (as defined in the National Initiative for Cybersecurity Education's coding structure); and

(ii) to assign the appropriate employment code to each such position, using agreed standards and definitions.

(2) CODE ASSIGNMENTS.—Not later than 1 year after the date after the procedures are established under paragraph (1)(E), the head of each Federal agency shall complete assignment of the appropriate employment code to each position within the agency with information technology, cybersecurity, or other cyber-related functions.

(c) PROGRESS REPORT.—Not later than 180 days after the date of enactment of this Act, the Director shall submit a progress report on the implementation of this section to the appropriate congressional committees.

**SEC. 304. IDENTIFICATION OF CYBER-RELATED ROLES OF CRITICAL NEED.**

(a) IN GENERAL.—Beginning not later than 1 year after the date on which the employment codes are assigned to employees pursuant to section 203(b)(2), and annually through 2022, the head of each Federal agency, in consultation with the Director, the Director of the National Institute of Standards and Technology, and the Secretary of Homeland Security, shall—

(1) identify information technology, cybersecurity, or other cyber-related roles of critical need in the agency's workforce; and

(2) submit a report to the Director that—

(A) describes the information technology, cybersecurity, or other cyber-related roles identified under paragraph (1); and

(B) substantiates the critical need designations.

(b) GUIDANCE.—The Director shall provide Federal agencies with timely guidance for identifying information technology, cybersecurity, or other cyber-related roles of critical need, including—

(1) current information technology, cybersecurity, and other cyber-related roles with acute skill shortages; and

(2) information technology, cybersecurity, or other cyber-related roles with emerging skill shortages.

(c) CYBERSECURITY NEEDS REPORT.—Not later than 2 years after the date of the enactment of this Act, the Director, in consultation with the Secretary of Homeland Security, shall—

(1) identify critical needs for information technology, cybersecurity, or other cyber-related workforce across all Federal agencies; and

(2) submit a progress report on the implementation of this section to the appropriate congressional committees.

**SEC. 305. GOVERNMENT ACCOUNTABILITY OFFICE STATUS REPORTS.**

The Comptroller General of the United States shall—

(1) analyze and monitor the implementation of sections 303 and 304; and

(2) not later than 3 years after the date of the enactment of this Act, submit a report to the appropriate congressional committees that describes the status of such implementation.

## TITLE IV—OTHER CYBER MATTERS

**SEC. 401. STUDY ON MOBILE DEVICE SECURITY.**

(a) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Secretary of Homeland Security, in consultation with the Director of the National Institute of Standards and Technology, shall—

(1) complete a study on threats relating to the security of the mobile devices of the Federal Government; and

(2) submit an unclassified report to Congress, with a classified annex if necessary, that contains the findings of such study, the recommendations developed under paragraph (3) of subsection (b), the deficiencies, if any, identified under (4) of such subsection, and the plan developed under paragraph (5) of such subsection.

(b) MATTERS STUDIED.—In carrying out the study under subsection (a)(1), the Secretary, in consultation with the Director of the National Institute of Standards and Technology, shall—

(1) assess the evolution of mobile security techniques from a desktop-centric approach, and whether such techniques are adequate to meet current mobile security challenges;

(2) assess the effect such threats may have on the cybersecurity of the information systems and networks of the Federal Government (except for national security systems or the information systems and networks of the Department of Defense and the intelligence community);

(3) develop recommendations for addressing such threats based on industry standards and best practices;

(4) identify any deficiencies in the current authorities of the Secretary that may inhibit the ability of the Secretary to address mobile device security throughout the Federal Government (except for national security systems and the information systems and networks of the Department of Defense and intelligence community); and

(5) develop a plan for accelerated adoption of secure mobile device technology by the Department of Homeland Security.

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

**SEC. 402. DEPARTMENT OF STATE INTERNATIONAL CYBERSPACE POLICY STRATEGY.**

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of State shall produce a comprehensive strategy relating to United States international policy with regard to cyberspace.

(b) ELEMENTS.—The strategy required by subsection (a) shall include the following:

(1) A review of actions and activities undertaken by the Secretary of State to date to support the goal of the President's International Strategy for Cyberspace, released in May 2011, to ''work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation.''.

(2) A plan of action to guide the diplomacy of the Secretary of State, with regard to foreign countries, including conducting bilateral and multilateral activities to develop the norms of responsible international behavior in cyberspace, and status review of existing discussions in multilateral fora to obtain agreements on international norms in cyberspace.

(3) A review of the alternative concepts with regard to international norms in cyberspace offered by foreign countries that are prominent actors, including China, Russia, Brazil, and India.

(4) A detailed description of threats to United States national security in cyberspace from foreign countries, state-sponsored actors, and private actors to Federal and private sector infrastructure of the United States, intellectual property in the United States, and the privacy of citizens of the United States.

(5) A review of policy tools available to the President to deter foreign countries, state-sponsored actors, and private actors, including those outlined in Executive Order 13694, released on April 1, 2015.

(6) A review of resources required by the Secretary, including the Office of the Coordinator for Cyber Issues, to conduct activities to build responsible norms of international cyber behavior.

(c) CONSULTATION.—In preparing the strategy required by subsection (a), the Secretary of State shall consult, as appropriate, with other agencies and departments of the United States and the private sector and nongovernmental organizations in the United States with recognized credentials and expertise in foreign policy, national security, and cybersecurity.

(d) FORM OF STRATEGY.—The strategy required by subsection (a) shall be in unclassified form, but may include a classified annex.

(e) AVAILABILITY OF INFORMATION.—The Secretary of State shall—

(1) make the strategy required in subsection (a) available the public; and

(2) brief the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives on the strategy, including any material contained in a classified annex.

**SEC. 403. APPREHENSION AND PROSECUTION OF INTERNATIONAL CYBER CRIMINALS.**

(a) INTERNATIONAL CYBER CRIMINAL DEFINED.—In this section, the term ''international cyber criminal'' means an individual—

(1) who is believed to have committed a cybercrime or intellectual property crime against the interests of the United States or the citizens of the United States; and

(2) for whom—

(A) an arrest warrant has been issued by a judge in the United States; or

(B) an international wanted notice (commonly referred to as a ''Red Notice'') has been circulated by Interpol.

(b) CONSULTATIONS FOR NONCOOPERATION.—The Secretary of State, or designee, shall consult with the appropriate government official of each country from which extradition is not likely due to the lack of an extradition treaty with the United States or other reasons, in which one or more international cyber criminals are physically present, to determine what actions the government of such country has taken—

(1) to apprehend and prosecute such criminals; and

(2) to prevent such criminals from carrying out cybercrimes or intellectual property crimes against the interests of the United States or its citizens.

(c) ANNUAL REPORT.—

(1) IN GENERAL.—The Secretary of State shall submit to the appropriate congressional committees an annual report that includes—

(A) the number of international cyber criminals located in other countries, disaggregated by country, and indicating from which countries extradition is not likely due to the lack of an extradition treaty with the United States or other reasons;

(B) the nature and number of significant discussions by an official of the Department of State on ways to thwart or prosecute international cyber criminals with an official of another country, including the name of each such country; and

(C) for each international cyber criminal who was extradited to the United States during the most recently completed calendar year—

(i) his or her name;

(ii) the crimes for which he or she was charged;

(iii) his or her previous country of residence; and

(iv) the country from which he or she was extradited into the United States.

(2) FORM.—The report required by this subsection shall be in unclassified form to the maximum extent possible, but may include a classified annex.

(3) APPROPRIATE CONGRESSIONAL COMMITTEES.—For purposes of this subsection, the term ''appropriate congressional committees'' means—

(A) the Committee on Foreign Relations, the Committee on Appropriations, the Committee on Homeland Security and Governmental Affairs, the Committee on Banking, Housing, and Urban Affairs, the Select Committee on Intelligence, and the Committee on the Judiciary of the Senate; and

(B) the Committee on Foreign Affairs, the Committee on Appropriations, the Committee on Homeland Security, the Committee on Financial Services, the Permanent Select Committee on Intelligence, and the Committee on the Judiciary of the House of Representatives.

**SEC. 404. ENHANCEMENT OF EMERGENCY SERVICES.**

(a) COLLECTION OF DATA.—Not later than 90 days after the date of enactment of this Act, the Secretary of Homeland Security, acting through the National Cybersecurity and Communications Integration Center, in coordination with appropriate Federal entities and the Director for Emergency Communications, shall establish a process by which a Statewide Interoperability Coordinator may report data on any cybersecurity risk or incident involving any information system or network used by emergency response providers (as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101)) within the State.

(b) ANALYSIS OF DATA.—Not later than 1 year after the date of enactment of this Act, the Secretary of Homeland Security, acting through the Director of the National Cybersecurity and Communications Integration Center, in coordination with appropriate entities and the Director for Emergency Communications, and in consultation with the Director of the National Institute of Standards and Technology, shall conduct integration and analysis of the data reported under subsection (a) to develop information and recommendations on security and resilience measures for any information system or network used by State emergency response providers.

(c) BEST PRACTICES.—

(1) IN GENERAL.—Using the results of the integration and analysis conducted under subsection (b), and any other relevant information, the Director of the National Institute of Standards and Technology shall, on an ongoing basis, facilitate and support the development of methods for reducing cybersecurity risks to emergency response providers using the process described in section 2(e) of the National Institute of Standards and Technology Act (15 U.S.C. 272(e)).

(2) REPORT.—The Director of the National Institute of Standards and Technology shall submit a report to Congress on the methods developed under paragraph (1) and shall make such report publically available on the website of the National Institute of Standards and Technology.

(d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to—

(1) require a State to report data under subsection (a); or

(2) require an entity to—

(A) adopt a recommended measure developed under subsection (b); or

(B) follow the best practices developed under subsection (c).

**SEC. 405. IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY.**

(a) DEFINITIONS.—In this section:

(1) BUSINESS ASSOCIATE.—The term ''business associate'' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(2) COVERED ENTITY.—The term ''covered entity'' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(3) HEALTH CARE CLEARINGHOUSE; HEALTH CARE PROVIDER; HEALTH PLAN.—The terms ''health care clearinghouse'', ''health care provider'', and ''health plan'' have the meanings given the terms in section 160.103 of title 45, Code of Federal Regulations.

(4) HEALTH CARE INDUSTRY STAKEHOLDER.—The term ''health care industry stakeholder'' means any—

(A) health plan, health care clearinghouse, or health care provider;

(B) patient advocate;

(C) pharmacist;

(D) developer of health information technology;

(E) laboratory;

(F) pharmaceutical or medical device manufacturer; or

(G) additional stakeholder the Secretary determines necessary for purposes of subsection (d)(1), (d)(3), or (e).

(5) SECRETARY.—The term ''Secretary'' means the Secretary of Health and Human Services.

(b) REPORT.—Not later than 1 year after the date of enactment of this Act, the Secretary shall submit, to the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Energy and Commerce of the House of Representatives, a report on the preparedness of the health care industry in responding to cybersecurity threats.

(c) CONTENTS OF REPORT.—With respect to the internal response of the Department of Health and Human Services to emerging cybersecurity threats, the report shall include—

(1) a clear statement of the official within the Department of Health and Human Services to be responsible for leading and coordinating efforts of the Department regarding cybersecurity threats in the health care industry; and

(2) a plan from each relevant operating division and subdivision of the Department of Health and Human Services on how such division or subdivision will address cybersecurity threats in the health care industry, including a clear delineation of how each such division or subdivision will divide responsibility among the personnel of such division or subdivision and communicate with other such divisions and subdivisions regarding efforts to address such threats.

(d) HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE.—

(1) IN GENERAL.—Not later than 60 days after the date of enactment of this Act, the Secretary, in consultation with the Director of the National Institute of Standards and Technology and the Secretary of Homeland Security, shall convene health care industry stakeholders, cybersecurity experts, and any Federal agencies or entities the Secretary determines appropriate to establish a task force to—

(A) analyze how industries, other than the health care industry, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries;

(B) analyze challenges and barriers private entities (notwithstanding section 102(15)(B), excluding any State, tribal, or local government) in the health care industry face securing themselves against cyber attacks;

(C) review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record;

(D) provide the Secretary with information to disseminate to health care industry stakeholders for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the health care industry;

(E) establish a plan for creating a single system for the Federal Government to share information on actionable intelligence regarding cybersecurity threats to the health care industry in near real time, requiring no fee to the recipients of such information, including which Federal agency or other entity may be best suited to be the central conduit to facilitate the sharing of such information; and

(F) report to Congress on the findings and recommendations of the task force regarding carrying out subparagraphs (A) through (E).

(2) TERMINATION.—The task force established under this subsection shall terminate on the date that is 1 year after the date of enactment of this Act.

(3) DISSEMINATION.—Not later than 60 days after the termination of the task force established under this subsection, the Secretary shall disseminate the information described in paragraph (1)(D) to health care industry stakeholders in accordance with such paragraph.

(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to limit the antitrust exemption under section 104(e) or the protection from liability under section 106.

(e) CYBERSECURITY FRAMEWORK.—

(1) IN GENERAL.—The Secretary shall establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, the National Institute of Standards and Technology, and any Federal agency or entity the Secretary determines appropriate, a single, voluntary, national health-specific cybersecurity framework that—

(A) establishes a common set of voluntary, consensus-based, and industry-led standards, security practices, guidelines, methodologies, procedures, and processes that serve as a resource for cost-effectively reducing cybersecurity risks for a range of health care organizations;

(B) supports voluntary adoption and implementation efforts to improve safeguards to address cybersecurity threats;

(C) is consistent with the security and privacy regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note) and with the Health Information Technology for Economic and Clinical Health Act (title XIII of division A, and title IV of division B, of Public Law 111–5), and the amendments made by such Act; and

(D) is updated on a regular basis and applicable to the range of health care organizations described in subparagraph (A).

(2) LIMITATION.—Nothing in this subsection shall be interpreted as granting the Secretary authority to—

(A) provide for audits to ensure that health care organizations are in compliance with the voluntary framework under this subsection; or

(B) mandate, direct, or condition the award of any Federal grant, contract, or purchase on compliance with such voluntary framework.

(3) NO LIABILITY FOR NONPARTICIPATION.—Nothing in this title shall be construed to subject a health care organization to liability for choosing not to engage in the voluntary activities authorized under this subsection.

**SEC. 406. FEDERAL COMPUTER SECURITY.**

(a) DEFINITIONS.—In this section:

(1) COVERED SYSTEM.—The term ''covered system'' shall mean a national security system as defined in section 11103 of title 40, United States Code, or a Federal computer system that provides access to personally identifiable information.

(2) COVERED AGENCY.—The term ''covered agency'' means an agency that operates a covered system.

(3) LOGICAL ACCESS CONTROL.—The term ''logical access control'' means a process of granting or denying specific requests to obtain and use information and related information processing services.

(4) MULTI-FACTOR LOGICAL ACCESS CONTROLS.—The term ''multi-factor logical access controls'' means a set of not less than 2 of the following logical access controls:

(A) Information that is known to the user, such as a password or personal identification number.

(B) An access device that is provided to the user, such as a cryptographic identification device or token.

(C) A unique biometric characteristic of the user.

(5) PRIVILEGED USER.—The term ''privileged user'' means a user who, by virtue of function or seniority, has been allocated powers within a covered system, which are significantly greater than those available to the majority of users.

(b) INSPECTOR GENERAL REPORTS ON COVERED SYSTEMS.—

(1) IN GENERAL.—Not later than 240 days after the date of enactment of this Act, the Inspector General of each covered agency shall submit to the appropriate committees of jurisdiction in the Senate and the House of Representatives a report, which shall include information collected from the covered agency for the contents described in paragraph (2) regarding the Federal computer systems of the covered agency.

(2) CONTENTS.—The report submitted by each Inspector General of a covered agency under paragraph (1) shall include, with respect to the covered agency, the following:

(A) A description of the logical access standards used by the covered agency to access a covered system, including—

(i) in aggregate, a list and description of logical access controls used to access such a covered system; and

(ii) whether the covered agency is using multi-factor logical access controls to access such a covered system.

(B) A description of the logical access controls used by the covered agency to govern access to covered systems by privileged users.

(C) If the covered agency does not use logical access controls or multi-factor logical access controls to access a covered system, a description of the reasons for not using such logical access controls or multi-factor logical access controls.

(D) A description of the following data security management practices used by the covered agency:

(i) The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.

(ii) What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including—

(I) data loss prevention capabilities; or

(II) digital rights management capabilities.

(iii) A description of how the covered agency is using the capabilities described in clause (ii).

(iv) If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.

(E) A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the data security management practices described in subparagraph (D).

(3) EXISTING REVIEW.—The reports required under this subsection may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the covered agency, and may be submitted as part of another report, including the report required under section 3555 of title 44, United States Code.

(4) CLASSIFIED INFORMATION.—Reports submitted under this subsection shall be in unclassified form, but may include a classified annex.

**SEC. 407. STRATEGY TO PROTECT CRITICAL INFRASTRUCTURE AT GREATEST RISK.**

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE AGENCY.—The term ''appropriate agency'' means, with respect to a covered entity—

(A) except as provided in subparagraph (B), the applicable sector-specific agency; or

(B) in the case of a covered entity that is regulated by a Federal entity, such Federal entity.

(2) APPROPRIATE AGENCY HEAD.—The term ''appropriate agency head'' means, with respect to a covered entity, the head of the appropriate agency.

(3) COVERED ENTITY.—The term ''covered entity'' means an entity identified pursuant to section 9(a) of Executive Order 13636 of February 12, 2013 (78 Fed. Reg. 11742), relating to identification of critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

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

(A) the Select Committee on Intelligence of the Senate;

(B) the Permanent Select Committee on Intelligence of the House of Representatives;

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

(D) the Committee on Homeland Security of the House of Representatives;

(E) the Committee on Energy and Natural Resources of the Senate;

(F) the Committee on Energy and Commerce of the House of Representatives; and

(G) the Committee on Commerce, Science, and Transportation of the Senate.

(5) SECRETARY.—The term ''Secretary'' means the Secretary of the Department of Homeland Security.

(b) STATUS OF EXISTING CYBER INCIDENT REPORTING.—

(1) IN GENERAL.—No later than 120 days after the date of the enactment of this Act, the Secretary, in conjunction with the appropriate agency head (as the case may be), shall submit to the appropriate congressional committees describing the extent to which each covered entity reports significant intrusions of information systems essential to the operation of critical infrastructure to the Department of Homeland Security or the appropriate agency head in a timely manner.

(2) FORM.—The report submitted under paragraph (1) may include a classified annex.

(c) MITIGATION STRATEGY REQUIRED FOR CRITICAL INFRASTRUCTURE AT GREATEST RISK.—

(1) IN GENERAL.—No later than 180 days after the date of the enactment of this Act, the Secretary, in conjunction with the appropriate agency head (as the case may be), shall conduct an assessment and develop a strategy that addresses each of the covered entities, to ensure that, to the greatest extent feasible, a cyber security incident affecting such entity would no longer reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

(2) ELEMENTS.—The strategy submitted by the Secretary with respect to a covered entity shall include the following:

(A) An assessment of whether each entity should be required to report cyber security incidents.

(B) A description of any identified security gaps that must be addressed.

(C) Additional statutory authority necessary to reduce the likelihood that a cyber incident could cause catastrophic regional or national effects on public health or safety, economic security, or national security.

(3) SUBMITTAL.—The Secretary shall submit to the appropriate congressional committees the assessment and strategy required by paragraph (1).

(4) FORM.—The assessment and strategy submitted under paragraph (3) may each include a classified annex.

**SEC. 408. STOPPING THE FRAUDULENT SALE OF FINANCIAL INFORMATION OF PEOPLE OF THE UNITED STATES.**

Section 1029(h) of title 18, United States Code, is amended by striking ''title if—'' and all that follows through ''therefrom.'' and inserting ''title if the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity organized under the laws of the United States, or any State, the District of Columbia, or other Territory of the United States.''.

**SEC. 409. EFFECTIVE PERIOD.**

(a) IN GENERAL.—Except as provided in subsection (b), this Act and the amendments made by this Act shall be in effect during the 10-year period beginning on the date of the enactment of this Act.

(b) EXCEPTION.—With respect to any action authorized by this Act or information obtained pursuant to an action authorized by this Act, which occurred before the date on which the provisions referred to in subsection (a) cease to have effect, the provisions of this Act shall continue in effect.

The PRESIDING OFFICER. The majority leader.

## MORNING BUSINESS

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

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

The Senator from Iowa.

## NATIONAL DOMESTIC VIOLENCE AWARENESS MONTH

Mr. GRASSLEY. Madam President, I think we have clearance on a noncontroversial resolution that is going to pass yet this evening, and I rise for about 5 minutes to speak on this issue.

Last week I submitted a resolution to commemorate the goals and ideals of National Domestic Violence Awareness Month, which takes place each October. I thank Senators LEAHY, AYOTTE, and KLOBUCHAR for joining me as original cosponsors of this measure.

I have met with many domestic violence victims over the years. We have come a long way since the enactment in 1984, with my support, of the landmark Family Violence Prevention and Services Act.

In the decades since then, Congress has committed billions of dollars to implement that statute, as well as the Violence Against Women Act, and we have seen a decline in the rate of serious partner violence over the last two decades, according to the Congressional Research Service.

But researchers and advocates who work with domestic violence survivors remind us that there is still much work to be done to stop this terrible crime and support survivors in their efforts to heal. It is estimated that as many as 9 million Americans are physically abused by a partner every year.

According to a 2011 survey by the Centers for Disease Control and Prevention, about 22 percent of women and about 14 percent of men have experienced severe physical abuse by a partner in their lifetime.

Experts tell us that domestic violence affects women, men, and children of every age and socioeconomic class, but we also know that women still experience more domestic violence than do men, and women are significantly more likely to be injured in an assault by a partner or a spouse.

According to the Justice Department's Bureau of Justice Statistics, women between the ages of 18 and 31 experience the highest rates of domestic violence. Most have been victimized by the same offender on at least one prior occasion. And, of course, it is heartbreaking to realize that millions of American children have been exposed to domestic violence, either by experiencing some form of abuse or witnessing a family member's abuse.

The good news is that each and every day, in communities across the Nation, there are victim advocates, service providers, crisis hotline staff and volunteers, as well as first responders who are working tirelessly to extend compassionate service to the survivors of domestic violence. I wish to take this opportunity to single out some of these folks and extend a special thank-you on behalf of the Senate.

First, I highlight the hard work of trained volunteers and staff who operate crisis hotlines across the country. They are a varied and talented group of individuals who, often at low or no pay, make confidential support, information, and referrals available to victims, as well as their friends and families, each and every day. We appreciate their efforts to help countless men, women, and children escape abusive situations.

Next, I recognize the contributions of the talented staff at the 56 State and territorial domestic violence coalitions around the country and the globe. These individuals also help respond to the needs of battered men, women, and children, typically by offering their expertise and technical support to local domestic violence programs in each and every State and territory. In my home State, for example, the Iowa State Coalition Against Domestic Violence has, since way back in 1985, connected local service providers to vitally important training and other resources that exist to support Iowa survivors.

We cannot commemorate Domestic Violence Awareness Month without also mentioning the police officers who are on the front lines in the effort to protect crime victims and to prevent abuse in the first place. Domestic violence calls can present lethal risks for officers, and we mourn those who have lost their lives while responding to such domestic violence incidents. We know, too, that in recent decades the law enforcement approach to these instances has changed to reflect the latest research, and we applaud those police agencies that continue to update and improve their domestic violence policies.

I also recognize those who operate the Nation's domestic violence shelters that meet the emergency housing needs of thousands of adults and children each day or millions of Americans each year. Last but not least, I want to highlight the hard work of the staff at charities and agencies across the Nation that are devoted to helping domestic violence survivors achieve financial independence, obtain legal assistance, and most importantly overcome the detrimental emotional and physical effects of abuse.

As I close, I urge my colleagues to support the adoption of this important resolution. With its adoption, we demonstrate the Senate supports the goals and ideals of National Domestic Violence Awareness Month.

I yield the floor.

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

Mr. WHITEHOUSE. Mr. President, I ask unanimous consent to speak for up to 20 minutes in morning business.

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

## CLIMATE CHANGE

Mr. WHITEHOUSE. Mr. President, there has been some activity on the Senate floor today regarding the President's Clean Power Plan, with fossil fuel State representatives coming to decry that plan. I would simply note that on October 22, in the Wall Street Journal, many of the leaders of America's national security took out an advertisement to say: ''Republicans & Democrats Agree: U.S. Security Demands Global Climate Action.''