RECESS

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

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

CYBERSECURITY ACT OF 2012—Continued

The PRESIDING OFFICER. The Senator from Maryland.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

I yield the floor.

I suggest the absence of quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The assistant bill clerk proceeded to call the roll.

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

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

The Senator from Wyoming.

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

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

SECOND OPINION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The assistant bill clerk proceeded to call the roll.

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

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

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

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

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

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

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

That was one example.

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

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

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

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

I said: What for?

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

I said: What do they do?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FOR-PROFIT COLLEGES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

I yield the floor.

The PRESIDING OFFICER. The Senator from Georgia.

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

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

REMEMBERING R. TIMOTHY STACK

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

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

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

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

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

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

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

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

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

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

I yield the floor.

The PRESIDING OFFICER. The Senator from Delaware is recognized.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Madam President, I yield the floor.

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

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

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

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

PRODUCTION TAX CREDIT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Madam President, I yield the floor.

The PRESIDING OFFICER. The Senator from Minnesota.

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

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

MEDICAL LOSS RATIO

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

I yield the floor.

The PRESIDING OFFICER. The Senator from Delaware.

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

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

The Senator from Maine.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The PRESIDING OFFICER. The Senator from Delaware.

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

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

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

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

The PRESIDING OFFICER. The Senator from Maine.

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

The PRESIDING OFFICER. The Senator from Delaware.

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

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

The PRESIDING OFFICER. The Senator from Connecticut.

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

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

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

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

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

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

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

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

I yield the floor.

The PRESIDING OFFICER. The Senator from Delaware.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

With that, I yield the floor.

The PRESIDING OFFICER. The Senator from Connecticut.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The PRESIDING OFFICER. The Senator from Nebraska.

THE FARM BILL

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

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

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

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

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

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

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

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

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

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

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

I yield the floor.

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

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

He went on:

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

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

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

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

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

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

The PRESIDING OFFICER. The clerk will call the roll.

The assistant legislative clerk proceeded to call the roll.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

I yield the floor.

The PRESIDING OFFICER. The Senator from Tennessee.

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

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

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

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

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

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

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

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

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

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

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

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

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

The Senator from Tennessee.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

AMENDMENT NO. 2731

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

The PRESIDING OFFICER. The clerk will report.

The bill clerk read as follows:

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

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

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

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The yeas and nays were ordered.

AMENDMENT NO. 2732 TO AMENDMENT NO. 2731

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

The PRESIDING OFFICER. The clerk will report.

The bill clerk read as follows:

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

The amendment is as follows:

At the end, add the following new section:

SEC. ___.

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

AMENDMENT NO. 2733

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

The PRESIDING OFFICER. The clerk will report.

The bill clerk read as follows:

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

The amendment is as follows:

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

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

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The yeas and nays were ordered.

AMENDMENT NO. 2734 TO AMENDMENT NO. 2733

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

The PRESIDING OFFICER. The clerk will report.

The bill clerk read as follows:

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

The amendment is as follows:

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

CLOTURE MOTION

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

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

The bill clerk read as follows:

CLOTURE MOTION

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

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

MOTION TO COMMIT WITH AMENDMENT NO. 2735

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

The PRESIDING OFFICER. The clerk will report the motion.

The bill clerk read as follows:

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

The amendment is as follows:

At the end, add the following new section:

SEC. _____.

This Act shall become effective 3 days after enactment.

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

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The yeas and nays were ordered.

AMENDMENT NO. 2736

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

The PRESIDING OFFICER. The clerk will report.

The bill clerk read as follows:

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

The amendment is as follows:

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

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

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The yeas and nays were ordered.

AMENDMENT NO. 2737 TO AMENDMENT NO. 2736

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

The PRESIDING OFFICER. The clerk will report.

The bill clerk read as follows:

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

The amendment is as follows:

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

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

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

VETERANS JOBS CORPS ACT OF 2012—MOTION TO PROCEED

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