

role in writing the rules, and if we step back and don't play a leadership role, some other nations will, but these are getting more and more complicated in this body.

Finally, something I feel very strongly about is that it is hard to face the world with this strong diplomatic might when there are a lot of ambassadorial positions that are vacant. Especially in the last 6 or 7 years we have seen efforts to block or delay ambassadorial appointments that have left key posts in many nations around the world vacant.

It sends a message to other countries. When they look at us, as the United States, not putting an ambassador in place, they basically conclude that the United States may not think we are important, and that is a very bad signal to send to other nations, especially when many nations that are allies have been without ambassadors for a while.

I am hoping we can reembrace on this 70th anniversary the wisdom of Truman, who said: The nation has to be vigorous and forceful and look toward diplomacy first.

With respect to the arrows of war—I am on the Armed Services Committee, and just like President Truman, I prefer diplomacy. I think we should lead with diplomacy, but we have to be willing to use military force. I voted for military force twice during my 3 years in the Senate.

In 2013, in August, the President asked us to vote for military force against Syria to punish Bashar al-Assad for using chemical weapons against civilians. The only vote that was taken in either House was a vote in the Senate Foreign Relations Committee. I voted for it with a kind of foreboding and heavy heart because I knew there would be Virginians, some of whom I might know, who would be affected, but nevertheless I thought it was an important principle for America to stand for.

Since September of 2014, I have also been pushing to have Congress cast a vote to authorize the war against ISIL that has been going on for 15 months. There is a lot of critique in this body—and I have critique—about the way that war is being waged about strategic decisions that the President is undertaking with respect to the war, but I think at the end of the day it is hard to just be a critic. Under article I of the Constitution, it is supposed to be Congress that authorizes war rather than a President just doing it on his own.

Earlier I mentioned how the Truman olive branches of diplomacy and arrows of war reinforce one another. Obviously, you can be a stronger negotiator at the table in advancing a diplomatic solution if people understand that you have significant military capacity and the willingness to use it in the appropriate instance. The more we can do and the better we can do to empower or military through wise budgeting, for example—as we hope to find an end to

sequester and a path forward—the stronger we will make our diplomatic effort. Similarly, the reverse is also true. The more we are vigorous in going after diplomacy, the more moral credibility we have in those instances where we can say, when looking at the world, looking at our citizens, and looking at our own troops, that we now think we need to take military action and we have exhausted the diplomatic alternatives first. That improves the moral credibility behind a military effort. It enables us to make the case better to all about the need for a military effort, and often it even creates a better international justification for a military effort.

I believe the Presiding Officer and I were together last week when former Secretary Gates testified before the Armed Services Committee. It was one of the best bits of testimony I have seen in my time in the Senate. He had a word of caution for us. He said: “While it is tempting to assert that the challenges facing the United States internationally have never been more numerous or complex, the reality is that turbulent, unstable and unpredictable times have recurred to challenge U.S. leaders regularly since World War II.”

We do live in a very complex and challenging world, where we see challenges that are known but also many unpredictable challenges. Other leaders of this country, since our first days, have lived in worlds that looked equally as challenging and confusing to them. We are true to our best traditions if the United States does what Truman so emblematically suggested we should do and we push in a vigorous and creative way all of the diplomatic tools at our disposal, and that involves diplomacy, but it also involves trade and humanitarian assistance. The United States is one of the most generous nations in the world.

The strength of our moral example is something that stands as so important. If you live in a nation where journalists are being put in jail, the U.S. freedom of the press stands as a moral example. If you live in a nation where people are prosecuted because of their sexual orientation, the United States stands as a great moral example. We are not exemplary in everything. We have room to improve in everything, but we are exemplary in so many things. People around the world still look at us, and that is in fact a diplomatic area of importance. Let's be exemplary and stand for the principles we expose.

Finally, I will say this. So many of the challenges we are facing now are challenges that at the end of the day are about diplomatic solutions. In the Armed Services or the Foreign Relations Committees, we are often talking about the vexing conundrum and humanitarian disaster in Syria, but at the end of the day we hear it has to be about a political solution to the civil war. There has to be a political solu-

tion to the conflict in Yemen. There has to be a political solution to the decades-long conflict between the Taliban and the Afghanistan Government. To find a political solution, you have to have strong diplomacy. Military action will not be enough to forge a political consensus moving forward.

Ultimately, this was the message of what Harry Truman did 70 years ago. This strong wartime President, who made some of the toughest decisions that have ever been made by anybody in the Oval Office, recognized that America was a great nation because when push came to shove, we would prefer, push, and advocate for diplomacy first knowing that we would be militarily strong if we needed to be. It is my hope that we in Congress will take a lesson from that anniversary and continue to pursue that same path.

With that, I yield the floor.

The PRESIDING OFFICER. The Senator from Maine.

Ms. COLLINS. Madam President, what is the pending business?

The PRESIDING OFFICER. We are in a period of morning business.

Ms. COLLINS. Madam President, I ask unanimous consent that I be permitted to speak for up to 15 minutes.

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

#### CYBERSECURITY INFORMATION SHARING BILL

Ms. COLLINS. Madam President, I rise to speak in favor of the Cybersecurity Information Sharing Act of 2015, and I urge my colleagues to support this much needed legislation. Nearly 3 months ago, the Senate was unable to find a path forward to adopt this important bill. Let's look at what has happened since the time that the Senate refused to proceed.

The fact is that our country has continued to endure a wave of damaging and expensive cyber attacks. These incidents include the first major hack of Apple's popular App Store, the compromise of 15 million T-Mobile users due to a breach at Experian, and the exposure of data of up to 8,000 Army families due to improper procedures followed by the General Services Administration. For the Army families who were affected, this sensitive information included medical histories, Social Security numbers, and child day care details.

Today, I renew my support for this bill in light of the continuing state of cyber insecurity that affects information held in the public and private sectors.

Passing the Cybersecurity Information Sharing Act would make it easier for public and private sector entities to share cyber threat information and vulnerabilities in order to lessen the theft of trade secrets, intellectual property, and national security information, as well as the compromise of sensitive personal information. It would eliminate some of the legal and

economic barriers impeding voluntary two-way information sharing between private industry and government. It is a modest but essential first step to protect networks and their information.

This bill would not in any way compromise our personal information. Its purpose is to help safeguard our personal information that breach after breach, cyber attack after cyber attack has proven to be vulnerable.

While this bill promotes appropriate information sharing between the government and the private sector—a good first step, as I have indicated—it unfortunately does little in its original form to harden the protection of Federal networks or to guard the critical infrastructure we rely upon every day. Thus, I have filed two amendments to further strengthen our Nation's cyber security.

The first amendment is directed at improving the security of sensitive personal data that is stored on networks of Federal civilian agencies. The insecurity of Federal databases and networks has been evident for years. Inspectors general reports have warned of it. Yet, by and large, those calls for action have not been heeded by Federal agencies, and certainly the weaknesses in our Federal agencies' security systems are underscored by recent breaches and intrusions.

In June, more than 20 million—20 million—current, former, and retired Federal employees learned that their personal data was stolen from the poorly secured databases of the Office of Personnel Management. Since that time, we have learned that the personal emails of the Director of the CIA have been hacked. We have learned from the State Department's inspector general that the State Department is “among the worst agencies in the Federal Government at protecting its computer networks.” This substandard performance at the Department of State continued even as an adversary nation breached the Department's email system last year. According to the IG, compliance with Federal information security standards remains “substandard” at the State Department.

I know from my many years of service on the committee on homeland security, where we worked on cyber security issues for literally a decade, producing legislation in 2010 and 2011 that unfortunately was not approved by this body, that this problem is long standing and it is only growing worse. We ignore it at our peril.

This appalling performance in so many agencies and departments led to my introducing bipartisan legislation with my colleague from Virginia, Senator WARNER, as well as Senator MIKULSKI, Senator COATS, Senator AYOTTE, and Senator MCCASKILL, to strengthen the security of the networks of Federal civilian agencies.

Our bill has five elements, but the most important provision would grant the Department of Homeland Security the authority to issue binding oper-

ational directives to Federal agencies to respond in the face of substantial breaches or to take action in the face of an imminent threat to a Federal network. Although the Secretary of Homeland Security is tasked with a very similar responsibility to protect Federal civilian networks, he has far less authority to accomplish this responsibility than does the Director of the National Security Agency for the dot-mil networks. We can no longer ignore the damaging consequences of failing to address these issues.

Our amendment would fortify Federal computer networks from cyber threats in many ways. The key elements, I am pleased to say, in our bill were incorporated into an amendment that has been filed by Senator CARPER, along with the chairman of the Homeland Security and Governmental Affairs Committee, Senator JOHNSON, and Senator WARNER, my chief cosponsor of the bill we introduced, and, of course, myself.

Our amendment has been included in the managers' substitute amendment, and I wish to thank Chairman BURR and Vice Chairman FEINSTEIN for their willingness to include these much needed provisions to boost the security of the networks at Federal civilian agencies.

Just think of the kind of data that civilian agencies have in the Federal Government. Whether we are talking about the Social Security Administration, the Medicare agency, the IRS, the VA or the Department of Defense, it is evident that millions of Americans—indeed, most Americans—have personal data, sensitive data, such as Social Security numbers, that are stored in these networks of Federal civilian agencies, and we have an obligation to protect as best we can that data.

I have also filed another amendment to the cyber bill, amendment No. 2623, that is aimed at protecting our country's most vital critical infrastructure from cyber attack. This bipartisan amendment was cosponsored by Senator COATS, Senator WARNER, and Senator HIRONO.

The livelihood and well-being of almost every American depend upon critical infrastructure that includes the electricity that powers our communities, the national air transportation system that moves passengers and cargo safely from one location to another, and the elements of the financial sector that ensure the \$14 trillion of payments made every day are securely routed through the banking system. Those are just some examples of critical infrastructure. There are obviously many more.

Our amendment would have created a second tier of mandatory reporting to the government for the fewer than 65 entities identified by the Department of Homeland Security where damage caused by a single cyber attack would likely result in catastrophic harm in the form of more than \$50 billion in economic damage, 2,500 fatalities or a

severe degradation of our national security. In other words, only cyber attacks that could cause catastrophic results would fall under this reporting requirement.

For 99 percent of businesses, the voluntary information sharing framework established in the bill before us would be enough, and the decision on whether or not to share cyber threat information should rightfully be left up to them. A second tier of reporting is necessary, however, to protect the critical infrastructure that is vital to the safety, health, and economic well-being of the American people.

Under our amendment, the owners and operators of the country's most critical infrastructure would report significant cyber attacks just as incidents of communicable disease outbreaks must be reported to public health authorities and to the Centers for Disease Control and Prevention.

Think about the situations we have here. Does it make sense that we require one case of measles to be reported to a Federal Government agency but not a cyber attack that could result in the death of more than 2,500 people? How does that make sense?

The threats to our critical infrastructure are not hypothetical. They are already occurring and increasing in frequency and severity. At a recent Armed Services Committee hearing on cyber security, Senator DONNELLY asked the Director of National Intelligence, Jim Clapper, what the No. 1 cyber challenge was that he was most concerned about. Director Clapper testified that, obviously, it was a large-scale cyber attack against the United States infrastructure.

In light of this No. 1 threat, how protected is our country? Well, I have posed that very question to the Director of the NSA, Admiral MIKE ROGERS. His answer, on a scale of 1 to 10, was that we are at about a 5 or 6. That is a failing grade when it comes to protecting critical infrastructure, no matter what curve we are grading on.

Although I am very disappointed that the Senate will not consider the original amendment I filed, I do want to acknowledge that Chairman BURR and Vice Chairman FEINSTEIN have worked closely with me on a compromise to begin to address the issue of cyber security risks that present such significant security threats to our critical infrastructure, and I am grateful for their acknowledging that this is a problem that deserves our attention.

This new amendment, which is section 407 of the managers' amendment, requires the DHS Secretary to conduct an assessment of the fewer than 65 critical infrastructure entities at greatest risk and develop a strategy to mitigate the risks of a catastrophic cyber attack. Let me stress two things. We are only talking about fewer than 65 entities that have already been designated by the Department of Homeland Security as critical infrastructure where a catastrophic cyber attack would cause terrible consequences.

Second, let me again describe what we mean by a catastrophic attack. It means a single cyber attack that would likely result in \$50 billion in economic damage, 2,500 Americans dying or a severe degradation of our national security. We are talking about significant consequences that would be catastrophic for this country—consequences we cannot and should not ignore.

There are plenty of cyber threats that cannot be discussed in public because they are classified—I know that as a member of the Senate Intelligence Committee—but in light of the cyber threat to critical infrastructure described by Admiral Rogers and Director of National Intelligence Clapper in open testimony before the Congress, the bare minimum we ought to do is to ask to require DHS and the appropriate Federal agencies to describe to us what more could be done to prevent a catastrophic cyber attack on our critical infrastructure.

One or two years from now, I don't want us to be standing here after a cyber 9/11 chastising ourselves, saying: Why didn't we do more to confront an obvious and serious threat to our critical infrastructure?

By including these two provisions in the managers' substitute amendment, we are strengthening the protections for Federal civilian agencies and beginning—not going nearly as far as I would like but beginning the vital task of protecting our critical infrastructure. We will be strengthening the cyber defenses of our Nation.

I urge my colleagues to support the managers' amendment and the underlying bill. By passing this long-overdue legislation, we will begin the long-overdue work of securing our economic and national security and our personal information for generations to come.

Thank you, Madam President.

I yield the floor.

Madam President, I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

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

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

#### TAKATA AIRBAG RECALL

Mr. NELSON. Madam President, I rise today to speak about the Takata airbag recall and the continued need for urgency in this area.

Last week the National Highway Traffic Safety Administration announced that they currently had—this figure will blow your mind—19 million vehicles and 23 million airbags under recall. So far, the completion rates for this recall are not very good. There is a national completion rate of some 22 percent, and for States such as Florida where there is high heat and humid-

ity—that is suspected as part of the reason the components break down—the completion rate is just under 30 percent, meaning that people are not taking their cars in to fix the problem that caused the recall in the first place.

Takata started running ads through the print media and social media, and Honda is running ads to get consumers to a dealer to replace their defective airbags. I am also aware that to boost replacement inflators, three other airbag manufacturers are helping to manufacture them.

So this Senator wants to take this opportunity to state that wherever this message can be delivered to consumers, you better take your car if it is under recall and get it in to the dealer in order to get a replacement airbag; otherwise, you are walking around with, in effect, a grenade in the middle of your steering wheel or dashboard.

Madam President, I ask unanimous consent to show a number of items in the Senate to illustrate what I am talking about with the airbags.

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

Mr. NELSON. To Members of the Senate, this is a deflated airbag that has already exploded. If you can see, this part is the center of the steering wheel. In this case, this happens to be a Honda; here is the letter "h." This would be sitting right in front of you in the steering wheel. When you have an accident, if it is of sufficient impact, it is going to cause the airbag to inflate. This is designed as a lifesaver. This explosive device inside the airbag, and the gas compound in there is ammonium nitrate. If it is defective, when the explosion occurs, the hot gases that are released from the compound come out through these little holes around the side, and that inflates the airbag. But what has happened and has caused almost 20 million cars to be recalled is that the hot gases are exploding in this device with such force that it is causing the metal to break and come out in the inflated bag with such force, tearing through the bag, as this particular bag shows—it has a big hole in it. Here is the hole where the metal came out. It is like a grenade exploding in front of you, in your steering wheel, with shrapnel going into the people who are driving or who are in the passenger seat with the dashboard airbag. We are finding out now that a few months ago there was the explosion of side airbags in some of the cars, in the doors. Lo and behold, that is throwing out shrapnel as well.

I want to show the Senate what it is like when these inflators explode. This is an inflator that was inside the device I just showed you. This photograph is a blowup by the Battelle Institute for the National Highway Traffic Safety Administration. This is a blown-up photograph of the inflator starting to inflate. What it is supposed to do is shoot the gases out here, which inflates the bag I showed you, but look what

has happened. It is being ruptured in the side, throwing out metal. This is what it looks like under very fast photography. Metal fragments are coming out when it should have been just gas coming out to inflate the bag.

This is what one of those pieces of metal looks like. It is a shard of metal that is part of the inflator. Can you imagine that hitting you in the neck? Well, that is what happened to one of my citizens in Florida, in the Orlando area. She ran into a fender bender in an intersection at a traffic light. Lo and behold, when the police got there, they found her slumped over the wheel, and they thought it was a homicide because her neck was slashed. They found out that what happened was a piece of metal like this had lacerated her neck and cut her jugular vein.

Another one of my constituents, a fireman—a big, hulking guy, the kind who will pick you up, if you are disabled and in a house that is burning down, and carry you out safely to save you—well, he won't be a fireman anymore because one of those metal fragments hit him in the eye and he is blind in one eye.

Those are just two incidents of scores across the country, of which there have been a handful of deaths.

If a jagged piece of metal can cause severe injury because it is coming at you at high speed, don't you think that if you have one of these vehicles that are under recall, you had better get it to the dealer to have it replaced?

Check to see if your car is under recall because sometimes people don't get it in the mail or they don't open the mail. Go to [www.safercar.gov](http://www.safercar.gov) and put in your car's vehicle identification number—the VIN number—and then you will see if your car is on a recall list.

Those that are on the recall list that I mentioned earlier unfortunately may not be the last to be recalled. The New York Times just reported that a study commissioned by Takata with Penn State University shows larger issues with the use of ammonium nitrate in the airbag inflators. In addition, there was another incident just this past June where a Takata side airbag ruptured in a relatively new 2015 Volkswagen. And just a week ago, General Motors recalled vehicles that also had defective Takata side airbags. It raises the question, are any of the Takata inflators safe?

Last week Senator THUNE and I sent a letter to Takata asking for additional documents and information regarding these side airbags. We also asked more questions about the use of ammonium nitrate. Also, the National Highway Traffic Safety Administration announced that it may expand its recall to all the model year vehicles with Takata airbags.

NHTSA must use all of its tools under the law to maximize consumer protection. These potential hand grenades, stored in the steering wheel or dashboard, must get off the road. The