On the National Day of Silence, we stand with our LGBT students to let them know that we understand, we care, and we are here for you.

I stand in silence to observe this day.

## COMMUNICATION FROM THE CLERK OF THE HOUSE

The SPEAKER pro tempore laid before the House the following communication from the Clerk of the House of Representatives:

OFFICE OF THE CLERK,
HOUSE OF REPRESENTATIVES,
*Washington, DC, April 18, 2013.*

Hon. JOHN A. BOEHNER,
*Speaker, U.S. Capitol, House of Representatives, Washington, DC.*

DEAR MR. SPEAKER: Pursuant to the permission granted in Clause 2(h) of Rule II of the Rules of the U.S. House of Representatives, the Clerk received the following message from the Secretary of the Senate on April 18, 2013 at 9:38 a.m.:

That the Senate agreed to S. Con. Res. 5.

Appointments:

Congressional Advisory Panel on the Governance of the Nuclear Security Enterprise.

With best wishes, I am

Sincerely,

KAREN L. HAAS.

## CYBER INTELLIGENCE SHARING AND PROTECTION ACT

Mr. SESSIONS. Mr. Speaker, I ask unanimous consent that during further consideration of H.R. 624 in the Committee of the Whole, pursuant to House Resolution 164, the last amendment in House Report 113–41 be modified in the form that I have placed at the desk.

The SPEAKER pro tempore. The Clerk will report the modification.

The Clerk read as follows:

Page 12, after line 18, insert the following:

Page 4, line 18, strike ''Federal Government'' and insert ''entities of the Department of Homeland Security and the Department of Justice designated under paragraphs (1) and (2) of section 2(b) of the Cyber Intelligence Sharing and Protection Act''.

Page 5, line 5, strike ''Federal Government'' and insert ''entities of the Department of Homeland Security and the Department of Justice designated under paragraphs (1) and (2) of section 2(b) of the Cyber Intelligence Sharing and Protection Act''.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Texas?

There was no objection.

GENERAL LEAVE

Mr. ROGERS of Michigan. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days to revise and extend their remarks and add extraneous material on the bill, H.R. 624.

The SPEAKER pro tempore (Mr. SESSIONS). Is there objection to the request of the gentleman from Michigan?

There was no objection.

The SPEAKER pro tempore. Pursuant to House Resolution 164 and rule XVIII, the Chair declares the House in the Committee of the Whole House on the state of the Union for the further consideration of the bill, H.R. 624.

Will the gentleman from California (Mr. DENHAM) kindly take the chair.

□ 1023

IN THE COMMITTEE OF THE WHOLE

Accordingly, the House resolved itself into the Committee of the Whole House on the state of the Union for the further consideration of the bill (H.R. 624) to provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, and for other purposes, with Mr. DENHAM (Acting Chair) in the chair.

The Clerk read the title of the bill.

The Acting CHAIR. When the Committee of the Whole rose on Wednesday, April 17, 2013, amendment No. 4 printed in House Report 113–41 offered by the gentleman from Rhode Island (Mr. LANGEVIN) had been disposed of.

AMENDMENT NO. 7 OFFERED BY MS. SINEMA

The Acting CHAIR. It is now in order to consider amendment No. 7 printed in House Report 113–41.

Ms. SINEMA. Mr. Chairman, I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 17, line 17, insert ''Department of Homeland Security and the Inspector General of the'' before ''Intelligence Community''.

Page 17, line 21, insert ''jointly and'' before ''annually''.

Page 17, line 22, strike ''congressional intelligence committees'' and insert ''the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the congressional intelligence committees''.

The Acting CHAIR. Pursuant to House Resolution 164, the gentlewoman from Arizona (Ms. SINEMA) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentlewoman from Arizona.

Ms. SINEMA. Mr. Chairman, I yield myself such time as I may consume.

My amendment is simple and straightforward. Currently, this bill, H.R. 624, requires the inspectors general of the intelligence community, Departments of Justice and Defense, as well as the Privacy and Civil Liberties Board to submit a report to Congress every year regarding the use of the information shared with the Federal Government. This amendment adds the inspector general of the Department of Homeland Security to the list of inspectors general that are required to submit the report.

It also adds the House and Senate Committees on Homeland Security to the list of committees that will receive the report. Currently, only the House and Senate Intelligence Committee will receive the report. Having the Department of Homeland Security, a civilian department, included in this reporting requirement adds one more layer of accountability to this review and report.

Allow me to briefly talk about the overall bill and why it has my support. I believe we need a 21st century solution for this 21st century problem. I've heard from businesses and constituents in Arizona who have firsthand knowledge of this issue. It's affecting both large corporations and small businesses alike. Our national security, our financial security, and our innovations are under very serious threat. This bill ensures that research and development, intellectual property, and software code is no longer being stolen by China, Iran, and Russia.

Countries and cyber hackers steal trade secrets and they steal innovation and research, but they also steal American jobs. Americans are known for their ingenuity and hard work, but we are losing that hard work to hackers. One of the biggest cyber threats is to an American's personal information—information like bank accounts, health records, and Social Security numbers.

This is very, very serious and a real threat to all Americans, and this threat is growing. Terrorist organizations have taken credit for taking down the online systems at Wells Fargo, JPMorgan Chase, and Bank of America. Three weeks ago, American Express also admitted that they were hacked.

Cyber attacks are becoming more sophisticated. Instead of merely disrupting commerce and stealing information, the attacks are focused on destroying our Nation's digital systems, destroying our national security, our infrastructure and financial systems that Americans depend on every day. It is imperative that we partner with private companies to discover, and then prevent, more attacks such as these.

I reserve the balance of my time.

Mr. ROGERS of Michigan. Mr. Chairman, while I do not oppose the amendment, I ask unanimous consent to control the time in opposition.

The Acting CHAIR. Without objection, the gentleman is recognized or 5 minutes.

There was no objection.

Mr. ROGERS of Michigan. I yield myself such time as I may consume.

Mr. Chair, I will support this amendment, and I want to thank the gentlelady from Arizona for her diligence and work in coming down to the briefings and getting well educated on the threat and familiarizing herself with the classified material. Thank you for your extra work on this issue, and thank you for being a strong voice in advocating our solution.

This amendment is important. It adds the inspector general at the Department of Homeland Security to the list of entities responsible for creating an annual report reviewing the use of information shared with the Federal Government. The amendment also adds the congressional Homeland Security Committee to the recipients of the report. This adds one more layer of oversight to make sure our civil liberties and privacy are protected in the bill.

I stand in support and appreciate all the efforts of the gentlelady from Arizona, and I reserve the balance of my time.

Ms. SINEMA. Mr. Chair, how much time do I have remaining?

The Acting CHAIR. The gentlewoman has 2½ minutes remaining.

Ms. SINEMA. Mr. Chair, I yield 2 minutes to the gentleman from New York (Mr. MAFFEI).

Mr. MAFFEI. I thank the gentlelady from Arizona for offering this amendment.

Mr. Chair, I rise today to speak in support of the Cyber Intelligence Sharing and Protection Act. I opposed the PATRIOT Act because many of its elements I did feel violated civil liberties and allowed things like profiling and abusive wiretapping; and while I don't think this was an easy decision, I do feel that this is certainly a different case.

Every day international agents, terrorists, and criminal organizations attack the public and private networks of the United States, as we speak. They disrupt services, attack newspapers and banks, infiltrate government agencies. They can steal intellectual property, and most alarmingly, they access private information of millions of citizens.

□ 1030

We've already seen state actors like the People's Republic of China pursue widespread data theft from American computer networks. Intelligence experts believe that rogue nations like Iran and even independent groups like WikiLeaks are pursuing very aggressive measures to hack into our Nation's power grid, our air traffic control systems, and individuals' personal financial records and other sorts of records across the country; and I do believe we should be very concerned. So while I do have some concern that the U.S. Government may access our private information in the cybersphere, I am more concerned that the Chinese Government will access our private information. This is a clear and present danger.

This bill does have protections that strictly prohibit the Federal Government from using or retaining any information other than for cyber threat purposes. And it remains illegal, after this bill is passed, for a company to share its information, except for cybersecurity reasons. This amendment will help to further enforce that.

We must recognize that cybersecurity threats are real and constantly changing. This bill is an important measure that allows private companies to share the cyber threat information with the Federal Government to help protect critical networks and infrastructure from attack.

I support this bill. It is an important step in our United States security strategy to protect our country from emerging cyber threats at home and abroad. And I support this amendment.

Mr. ROGERS of Michigan. Mr. Chairman, I yield such time as he might consume to the gentleman from Maryland (Mr. RUPPERSBERGER).

Mr. RUPPERSBERGER. I thank the chairman for yielding.

First thing, to the Congresswoman from Arizona, I really appreciate all of your work on this bill. You came to Congress; you did your homework; you decided that it was important to protect our country; and you've done a lot of work. I just want to let you know that you've done a great job for your district and for America, generally, and I want to thank you for that.

Basically, this amendment really allows the Committee on Homeland Security and the Inspector General to oversee and to do reporting. It's important that we have oversight. I know the chairman and I have worked hard to make sure that we deal with all of the privacy issues, and this is just another example of how we're going to protect our privacy. You cannot have security if you don't have privacy.

Ms. SINEMA. Mr. Chairman, I just want to emphasize again that this amendment helps add another layer of accountability. It includes the Homeland Security Department as a civilian interface for Congress in both the Homeland Security Committee and the Intelligence Committee.

I want to thank, in particular, the chair and the ranking member for their leadership on this issue over the course of several years. I know in my district it's important not just to consumers, but also to industry leaders who are leading the way forward on American innovation. I want to thank them for that.

I encourage Members to support this amendment, and I yield back the balance of my time.

Mr. ROGERS of Michigan. I yield back the balance of my time, Mr. Chairman.

The Acting CHAIR. The question is on the amendment offered by the gentlewoman from Arizona (Ms. SINEMA).

The question was taken; and the Acting Chair announced that the ayes appeared to have it.

Ms. SINEMA. Mr. Chairman, I demand a recorded vote.

The Acting CHAIR. Pursuant to clause 6 of rule XVIII, further proceedings on the amendment offered by the gentlewoman from Arizona will be postponed.

AMENDMENT NO. 8, AS MODIFIED, OFFERED BY MS. LORETTA SANCHEZ OF CALIFORNIA

The Acting CHAIR. It is now in order to consider amendment No. 8 printed in House Report 113–41.

Ms. LORETTA SANCHEZ of California. Mr. Chairman, I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 18, beginning on line 24, strike ''Director of National Intelligence and'' and insert ''Director of National Intelligence,''.

Page 19, line 1, insert ''and the Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland,'' after ''Justice,''.

The Acting CHAIR. Pursuant to House Resolution 164, the gentlewoman from California (Ms. LORETTA SANCHEZ) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentlewoman from California.

Ms. LORETTA SANCHEZ of California. Mr. Chairman, I yield myself such time as I may consume.

Mr. Chairman, the challenge of defending our Nation on a constantly expanding cyber front continues to grow. I believe that I'm one of those Members of the Congress that sits both on the House Armed Services Committee and on the Homeland Security Committee and I see it from both angles, both from the civilian side and the military side.

I've constantly tried to improve how we address the need for the next-generation technology, public-private cooperation, and ensuring that we have the right personnel to counter this 21st-century cyber threat. However, I am uncompromising in safeguarding the rights of our citizens, and I will never sacrifice our civil liberties for unneeded intrusion.

To this end, the amendment I am offering today would strengthen existing provisions in the bill to include the Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security as key stakeholders in the report that would assess the impact activity caused by this legislation.

This report would assess how this legislation affected our civil liberties and privacy throughout our Federal Government. The Department of Homeland Security is ''the'' key civil Department in our Federal Government that develops and implements cybersecurity protocols for the rest of the Federal Government. It's crucial that they be part of any civil liberty and privacy assessment.

I have worked closely with both the Privacy Office and the Office of Civil Rights and Civil Liberties. The individuals in these offices are experts in their fields and they should have a say; they should be in the room as we take a look at this.

Much work needs to be done, but I urge my colleagues to support my amendment to continue improving this bill.

I reserve the balance of my time.

Mr. ROGERS of Michigan. Mr. Chairman, while I do not oppose the amendment, I ask unanimous consent to control the time in opposition.

The Acting CHAIR. Without objection, the gentleman is recognized for 5 minutes.

There was no objection.

Mr. ROGERS of Michigan. Mr. Chairman, I will support this amendment; and I want to thank the gentlelady for her work and interest on this very,

very important issue and her taking the time to be involved in the process of making this a better bill and protecting privacy and civil liberties.

What this bill does is add a Privacy Officer and Officer of Civil Rights and Civil Liberties of the Department of Homeland Security to the list of entities responsible for producing an annual report assessing the privacy and civil liberties impact of activities conducted by the Federal Government under this bill.

Because the bill requires the Senior Privacy and Civil Liberties Officer of each department or agency receiving information under the bill to participate in the report, I will not oppose this effort to specifically include these officials from the Department of Homeland Security.

I think this is, again, making more clarification, making our privacy and civil liberties protection that much more robust in the bill, and I want to thank the gentlelady for her efforts.

With that, Mr. Chairman, I reserve the balance of my time.

Ms. LORETTA SANCHEZ of California. Mr. Chairman, I thank the kind chairman for his remarks and his support.

Mr. Chairman, I ask unanimous consent that the amendment be modified with the modification that is at the desk.

The Acting CHAIR. The Clerk will report the modification.

The Clerk read as follows:

Insert ''Security'' after ''Homeland'' in the second instruction.

The Acting CHAIR. Is there objection to the request of the gentlewoman from California?

There was no objection.

The Acting CHAIR. The amendment is so modified.

Ms. LORETTA SANCHEZ of California. Mr. Chairman, I yield 1 minute to my good friend, the gentleman from California (Mr. MCNERNEY).

Mr. MCNERNEY. I thank my colleague from California, and I rise in support of Ms. SANCHEZ's amendment, but in opposition to the underlying bill, H.R. 624.

This legislation has positive aspects, but I'm concerned with the civil protections not required in H.R. 624. Ms. SANCHEZ's amendment is a necessary step toward improving the bill by giving oversight authority to a civilian agency.

Sharing information is absolutely essential; however, in exchange for the liabilities protections given to businesses that share cyber threat information with the government, it is our responsibility here in Congress to protect our constituents' private information. Businesses should be required to remove personally identifiable information before submitting data to Federal agencies.

I thank Ms. SANCHEZ again for her efforts, as well as Mr. ROGERS and Mr. RUPPERSBERGER for their efforts as leaders of the Intelligence Committee.

Mr. ROGERS of Michigan. I would thank the gentlelady again and yield back the balance of my time.

Ms. LORETTA SANCHEZ of California. Mr. Chairman, I yield back the balance of my time.

The Acting CHAIR. The question is on the amendment, as modified, offered by the gentlewoman from California (Ms. LORETTA SANCHEZ).

The amendment was agreed to.

AMENDMENT NO. 9 OFFERED BY MR. LAMALFA

The Acting CHAIR. It is now in order to consider amendment No. 9 printed in House Report 113–41.

Mr. LAMALFA Mr. Chairman, I have an amendment at the desk made in order under the rule.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 22, after line 7 insert the following:

''(7) LIMITATION ON SURVEILLANCE.—Nothing in this section shall be construed to authorize the Department of Defense or the National Security Agency or any other element of the intelligence community to target a United States person for surveillance.

The Acting CHAIR. Pursuant to House Resolution 164, the gentleman from California (Mr. LAMALFA) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from California.

□ 1040

Mr. LAMALFA. I yield myself such time as I may consume.

Mr. Chair, I appreciate the opportunity to rise today and speak in favor of my amendment to the Cyber Intelligence Sharing and Protection Act. This is an example of the process working. A lot of folks have expressed concerns about the measure here, not only on the cyber intelligence side but as well the privacy and personal security side. I think this amendment and many others that we have seen today, and will see, are addressing that issue so we get the right balance between cybersecurity and individual liberties and freedoms, Fourth Amendment concerns.

The threat we face today in the cyber realm is nothing short of a serious threat to our national security. Nation-states like China and Russia are targeting the American government and the American private sector alike for cyber espionage, and potentially for cyber attack.

Chinese espionage targeting the American private sector to steal core research and development information—at the very heart of American innovations and jobs—represents an unprecedented threat to our very way of life.

While strongly supporting this legislation, I am pleased to have worked with Chairman ROGERS and Ranking Member RUPPERSBERGER to further clarify that nothing in the legislation should be construed to be a surveillance program directed at American citizens.

The amendment is very concise yet extremely important. Titled the ''Limitation on Surveillance,'' it simply reads as follows:

Nothing in this section shall be construed to authorize the Department of Defense or the National Security Agency or any other element of the intelligence community to target a United States person for surveillance.

As we act to protect the United States from cyber attack by foreign countries and terrorist groups, we must ensure that our constitutional rights and privacy are maintained. The term ''United States person'' includes U.S. citizens and legal residents or legal visitors to the country, limiting the surveillance powers of this bill to foreign nationals and those entering the Nation illegally.

This amendment helps to strike the balance this measure strives for, granting our government the means to defend the Nation while, importantly, preventing any inappropriate use of these powers.

Again, I am pleased to support legislation that creates no new regulatory regime and does not create additional Federal bureaucracy or require significant additional spending.

I reserve the balance of my time.

Mr. RUPPERSBERGER. Mr. Chair, I rise to claim time in opposition, even though I am not opposed to the amendment.

The CHAIR. Without objection, the gentleman from Maryland is recognized for 5 minutes.

There was no objection.

Mr. RUPPERSBERGER. Mr. Chair, while we never believe that any surveillance of Americans was permitted under our bill, we are taking any and all precautions to make it entirely clear that no element of the intelligence community—which, of course, includes the Department of Defense and the National Security Agency—is authorized to target any United States person for surveillance. The chairman's amendment solidifies the privacy and civil liberties protections that we always have intended to have as part of the bill. No American activities or communications will be targeted—period. We cannot have security without privacy.

Therefore, I urge a ''yes'' vote on this amendment, and I reserve the balance of my time.

Mr. LAMALFA It is my pleasure to now yield 1 minute to the chairman of the Intel Committee, the gentleman from Michigan (Mr. ROGERS).

Mr. ROGERS of Michigan. Mr. Chair, I support this amendment, which makes very, very clear that nothing in this bill authorizes the government to target an American citizen for surveillance. It's incredibly important.

Though the underlying bill would not allow the surveillance of an American citizen under CISPA, I will support this amendment as a further clarification that settles some Members' concerns and ensures the scope of the bill stays as narrow as we intended it to be.

The amendment is an important myth buster about the intentions of CISPA. I commend Mr. LAMALFA for his leadership on this issue and urge strong support for the LaMalfa amendment.

Mr. RUPPERSBERGER. I would like to yield to the gentleman from Virginia, the chairman of the Judiciary Committee, Congressman GOODLATTE, as much time as he may consume. And I would also like to thank him personally for working closely with us on this bill to have a bill that will protect the citizens of the United States of America.

Mr. GOODLATTE. I thank the gentleman from Maryland, the ranking member, for not only yielding me this time, but also for the great work that he has done, and also the great work that Chairman ROGERS has done. They have worked together in a bipartisan fashion to accomplish something very, very important to accomplish in terms of fighting cyber terrorism, cyber crime, and making sure that we are safe in this country from cyber attacks to which we are very vulnerable today.

I also want to thank the gentleman from California for his amendment. I support efforts to make it absolutely clear that this legislation does not in any way authorize the surveillance of American citizens.

I also want to thank Chairman ROGERS and Ranking Member RUPPERSBERGER for working with me to enhance the liability provisions in the legislation, for working with me to address some jurisdictional issues in the bill that affected the Department of Justice and the House Judiciary Committee.

I would also like to note that the President's statement in opposition to this bill insists on exposing our best technology providers to even more lawsuits when they are simply helping to defend our Nation against cyber attacks. The President's opposition statement expresses a deep distrust of private industry that America has rejected since its founding.

The bill before us today instead welcomes the private sector and acknowledges that we need the best minds in the country to help protect our citizens from ever-evolving cyber attacks by the likes of China and Iran. And the work done by the chairman and the ranking member to improve the provision of this bill, working with my committee and my staff to make it clear that we have a definite definition of what constitutes good faith and what constitutes circumstances under which a business that does not act in good faith would be exposed to lawsuits and liability, is one that helps protect the privacy of American citizens, because those citizens will be assured they will know under what circumstances a business has exceeded its authority under the law and be protected and have a clear right to bring an action under those circumstances. And the businesses themselves will be protected because they will not share information if they know they are not acting in good faith, because they know what the definition of good faith is in the bill.

So the gentleman from Michigan, the gentleman from Maryland, the chairman and ranking member, have done a great job with this legislation. I support their efforts and urge my colleagues to do the same.

Mr. LAMALFA Mr. Chair, again, thank you to my colleagues. The ranking member from Maryland (Mr. RUPPERSBERGER), I really appreciate your kind words and your strong support. To my colleague from Virginia, thank you for your kind words on the amendment as well. And to my colleague, Mr. Chairman, Mr. ROGERS from Michigan, thank you for letting me offer this amendment here.

It does strike the balance I think we need with cybersecurity. The great threat to many of our institutions in this Nation is something that we do have to act upon, but also finding that balance with personal privacy that is so key to the elements of the founding of our Nation. I'm proud to be able to carry this amendment. I ask for your support, Mr. Chairman, and I yield back the balance of my time.

Mr. RUPPERSBERGER. I yield back the balance of my time.

The Acting CHAIR. The question is on the amendment offered by the gentleman from California (Mr. LAMALFA).

The question was taken; and the Acting Chair announced that the ayes appeared to have it.

Mr. ROGERS of Michigan. Mr. Chair, I demand a recorded vote.

The Acting CHAIR. Pursuant to clause 6 of rule XVIII, further proceedings on the amendment offered by the gentleman from California will be postponed.

□ 1050

AMENDMENT NO. 10 OFFERED BY MR. PAULSEN

The Acting CHAIR. It is now in order to consider amendment No. 10 printed in House Report 113–41.

Mr. PAULSEN. I offer an amendment, Mr. Chair.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

At the end of the bill, add the following new section:

**SEC. 4. SENSE OF CONGRESS ON INTERNATIONAL COOPERATION.**

It is the sense of Congress that international cooperation with regard to cybersecurity should be encouraged wherever possible under this Act and the amendments made by this Act.

The Acting CHAIR. Pursuant to House Resolution 164, the gentleman from Minnesota (Mr. PAULSEN) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Minnesota.

Mr. PAULSEN. Mr. Chair, I yield myself such time as I may consume.

Mr. Chair, last month at a Senate hearing outlining the threats facing our security, it was the Director of National Intelligence, James Clapper, who warned that the intelligence community is seeing indications that some terror groups are interested in ''developing offensive cyber capabilities, and cyber criminals are using a growing black market to sell cyber tools that fall into the hands of both state and nonstate actors.''

Mr. Chair, just last week in Chairman ROGERS' committee, it was Director Clapper who also said, ''As more and more state and nonstate actors gain cyber expertise, its importance and reach as a global threat cannot be overstated.''

Our society has increasingly become reliant on modern technology in nearly every aspect of our daily lives, making the possibility of a cyber attack that much more dangerous. Under cyber terrorist or cyber crime, industries as diverse as financial systems, transportation, social media, and even utilities could be negatively impacted. A successful attack could disrupt the lives of Americans and result in other unpredictable consequences.

We do know the threat is real. We've already experienced attacks on our Nation's financial institutions and have faced hackers trying to gain access to the Pentagon and our Nation's critical infrastructure. According to the U.S. Government Accountability Office, the number of U.S. organizations believed to have been hacked has dramatically increased in just the last 6 years. Back in 2006, there were about 5,500 separate attacks noted, compared to 48,500 in 2012. As a January 2013 U.S. Government report found, cyber attacks and intrusions in critical energy infrastructures rose 52 percent between 2011 and 2012 alone. That's in a 1-year period, Mr. Chair.

Cyber weapons will likely continue to be used by a greater number of countries and other actors as a form of warfare. Between 20 and 30 states already have the capability to launch cyber warfare, including China, Russia, Iran, and North Korea and others, as has been stated as part of the debate on this bill.

Fortunately, these attacks have so far been thwarted by our intelligence before significant and lasting damage could occur, but it would be unwise to choose to act alone in the face of the growing fact of cyber criminality. In order to produce effective outcomes, our intelligence community must continue to promote collaboration among experts and across boards.

Just as we conduct our drills and our training exercises with our allies, we need to work together to share our best practices to keep our citizens safe from cyber attacks. My amendment would call on Congress to encourage international cooperation when it comes to cybersecurity.

This amendment would not bind the United States to working with other

nations, but it simply does promote doing so in situations that would be mutually beneficial. Such collaboration would more effectively allow us to combat cyber terrorism and threats by sharing resources and using proven security techniques when possible.

Mr. Chair, in the end, by working together on an issue that poses a threat to all of us, the international community will benefit from the exchange of experiences and potential solutions.

Mr. Chair, I just want to thank the gentleman from Michigan and the gentleman from Maryland for their leadership on this very challenging issue. I know that looking forward we will continue to see success in battling these real threats.

With that, I reserve the balance of my time.

Mr. RUPPERSBERGER. I rise to claim the time in opposition to this amendment even though I'm not opposed.

The Acting CHAIR. The gentleman from Maryland is recognized for 5 minutes.

Mr. RUPPERSBERGER. I thank Congressman PAULSEN for his work on this bill. I support his amendment with the sense of Congress to encourage international cooperation with regard to cybersecurity whenever possible under this bill.

Given that cyber threats are global in nature, as are our networks and computer systems, international efforts must work together to protect against domestic and foreign actors who seek to destroy our industries, government, agencies, and utilities.

Therefore, I urge a ''yes'' vote on the amendment, and I yield back the balance of my time.

Mr. PAULSEN. Mr. Chair, I yield such time as he may consume to the committee chairman.

Mr. ROGERS of Michigan. Mr. Chairman, I support this amendment and agree that we must employ international cooperation to combat the scourge of economic cyber espionage and leverage our official state relationships and alliances to help stop the bleeding.

China's economic espionage has reached an intolerable level, and I believe U.S. officials should demand that it stop at every meeting and engagement we have with Chinese officials. Moreover, the United States and our allies in Europe and Asia have an obligation to confront Beijing and demand they put a stop to this piracy.

Beijing is waging a massive trade war on us all, and we should band together to pressure them to stop. Combined, the United States and our allies in Europe and Asia have significant diplomatic and economic leverage over China, and we should use this to our advantage to put an end to this activity.

I commend the gentleman from Minnesota for offering this amendment, and I urge my colleagues' strong support for it.

Mr. PAULSEN. Mr. Chair, I urge support for my amendment, and I yield back the balance of my time.

The Acting CHAIR. The question is on the amendment offered by the gentleman from Minnesota (Mr. PAULSEN).

The amendment was agreed to.

AMENDMENT NO. 11 OFFERED BY MR. BARTON

The Acting CHAIR. It is now in order to consider amendment No. 11 printed in House Report 113–41.

Mr. BARTON. Mr. Chair, I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

At the end of the bill, add the following new section:

**SEC. 4. RULE OF CONSTRUCTION RELATING TO CONSUMER DATA.**

Nothing in this Act or the amendments made by this Act shall be construed to provide new or alter any existing authority for an entity to sell personal information of a consumer to another entity for marketing purposes.

The Acting CHAIR. Pursuant to House Resolution 164, the gentleman from Texas (Mr. BARTON) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Texas.

Mr. BARTON. Mr. Chair, I yield myself such time as I may consume.

(Mr. BARTON asked and was given permission to revise and extend his remarks.)

Mr. BARTON. Mr. Chair, when this same bill or bill similar to it was on the House floor last year, I had to reluctantly rise in opposition to it because it was my opinion that the privacy protections in the bill were not sufficient to protect the privacy of the American people. I think that surprised a lot of people that I was not for the bill.

After the bill failed to move in the Senate, I went to Chairman ROGERS and I told him that I supported the underlying intent of the bill and I was hopeful that, if the bill came back up in this session, he and myself and our staffs could work together to improve the privacy protections. He promised then that he would do it, and Chairman ROGERS and his staff have been men and women of their word. The result is a bill that was reported out of the Intelligence Committee on a bipartisan basis with much stronger privacy protections.

When I went to the Rules Committee, Chairman ROGERS supported that this amendment I'm about to offer should be made in order, and it has been. And if this amendment is accepted—and I'm told that the chairman and the ranking member are going to support it, as I'm not aware of any organized opposition to it—it is going to be my intent to vote for the bill.

We obviously have a cyber threat that faces the American people, and Chairman ROGERS and Ranking Member RUPPERSBERGER have talked about that in some detail earlier in this debate. We want to combat that threat. But in doing it, we do not want to eliminate or weaken the privacy protections of the American people that we represent in this body.

So what my amendment does is make sure that any information that is collected is going to be used simply for the purpose of protecting against cyber threats. It's a very short amendment. It adds a new section to the bill, section 4. Here I will read the amendment since it's in clear English and very short.

Nothing in this act or the amendments made by this act shall be construed to provide new or alter any existing authority for an entity to sell personal information of a consumer to another entity for marketing purposes.

What this does, Mr. Chair, is simply nail down the fact that when we find information that might be necessary to protect against a cyber threat, that's all it's going to be used for. It can't be used for any other purpose.

As I said earlier, Chairman ROGERS has worked very closely with myself, and his staff has worked with my staff. Congressman MARKEY of Massachusetts, who is the cochairman of the Privacy Caucus, strongly supports this amendment.

Again, I think it was unanimously accepted at the Rules Committee. I'm aware of no opposition, so I hope that we can adopt the amendment.

With that, I reserve the balance of my time.

□ 1100

Mr. RUPPERSBERGER. I rise to claim the time in opposition even though I am not opposed to the amendment.

The Acting CHAIR. Without objection, the gentleman from Maryland is recognized for 5 minutes.

There was no objection.

Mr. RUPPERSBERGER. First, I would like to thank Congressman BARTON for his work on the bill.

You've made the bill stronger, and we want to make sure that there is no perception that people's privacies are being violated.

I support Congressman BARTON's amendment, which ensures that nothing in our bill, CISPA, provides the authority for any entity to sell a consumer's personal information for marketing purposes.

I yield back the balance of my time.

Mr. BARTON. I yield such time as he may consume to the distinguished chairman of the Intelligence Committee and also a distinguished member of the Energy and Commerce Committee, a former FBI agent, the gentleman from Michigan (Mr. ROGERS).

Mr. ROGERS of Michigan. Thank you, Mr. BARTON, for your work on this.

Last year, you expressed strong reservations about certain privacy protections, and you were willing to sit down and work with us to try to find and make sure that we sent that very clear

message about protecting privacy in this bill. I thought the language was excellent, and it added to that purpose. It really does prevent any information in the bill from being misused by a company for anything other than the bill's strictly defined cybersecurity purpose. But his amendment adds an important clarification to make Congress' intent absolutely clear, to try again to reassure the American public that this is about protecting privacy and civil liberties while protecting the country.

I want to thank Mr. BARTON for working with me and my ranking member on this important issue, and I urge my colleagues to strongly support this amendment.

Mr. BARTON. In reclaiming my time, Mr. Chairman, before I yield back, I want to thank my staff member Emmanual Guillory. He has worked tirelessly on this issue and on this amendment. I also want to thank Congressman ED MARKEY of Massachusetts and his staff for working with me and Chairman ROGERS and Ranking Member RUPPERSBERGER.

With that, I yield back the balance of my time.

The Acting CHAIR. The question is on the amendment offered by the gentleman from Texas (Mr. BARTON).

The amendment was agreed to.

AMENDMENT NO. 12 OFFERED BY MS. JACKSON LEE

The Acting CHAIR. It is now in order to consider amendment No. 12 printed in House Report 113–41.

Ms. JACKSON LEE. Mr. Chair, I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

At the end of the bill, add the following new section:

**SEC. 4. SAVINGS CLAUSE WITH REGARD TO CYBERSECURITY PROVIDER OBLIGATION TO REPORT CYBER THREAT INCIDENT INFORMATION TO FEDERAL GOVERNMENT.**

Nothing in this Act or the amendments made by this Act shall be construed to provide authority to a department or agency of the Federal Government to require a cybersecurity provider that has contracted with the Federal Government to provide information services to provide information about cybersecurity incidents that do not pose a threat to the Federal Government's information.

The Acting CHAIR. Pursuant to House Resolution 164, the gentlewoman from Texas (Ms. JACKSON LEE) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentlewoman from Texas.

Ms. JACKSON LEE. Let me thank the chairman and the ranking member for the work that they have done in getting us here today and in crafting the legislation, and I thank the Rules Committee for making what I think is a very important amendment in order. I thank this process for allowing clarifying amendments because we are here representing the American people.

Mr. Chair, my amendment is straightforward. It improves the bill by indicating that:

Nothing in this Act or the amendments made by this Act shall be construed to provide authority to a department or agency of the Federal Government to require a cybersecurity provider that has contracted with the Federal Government to provide information services to provide information about cybersecurity incidents that do not pose a threat to the Federal Government.

We want to be concerned about that.

It makes it clear that the only instance in which a cloud service provider can share information about a cyber incident with a government agency is when the objective of an attempted intrusion of the service provider's network was to gain unauthorized access to the government's information.

I am pleased to state that this commonsense amendment is supported by a number of groups, including Constitutional Alliance, The Constitution Project, Liberty Coalition, and the ACLU.

In other words, if a cyber incident does not threaten the government's information, then the incident is none of the government's need to intrude, and this is especially true when disclosure to the government would compromise an individual's privacy and proprietary information of businesses.

Mr. Chairman, today, something commonly called the ''cloud'' plays an unseen but critical part in the lives of millions of Americans and thousands of businesses. Persons and businesses that use iPhones, Gmail, Yahoo!, and MSN email services are connected to the cloud. This, of course, does not in any way hinder our homeland security or national security. Cloud services include popular online services like Facebook and YouTube. The cloud is saving consumers and businesses from the loss of valuable data through storage services, and when you speak to our industries, they are protected.

This is the cloud—all private sector. They are not intruded upon, but add the government—if the government comes in and decides just without any clarification that we'll give your information to others without it being necessary, without it being government information, without it being related to government operations, my amendment protects you in the private sector from that kind of intrusion.

So I believe that this amendment will protect commerce. These are well-known names. This is who this amendment will protect—all of those who are generating commerce in the midst of cloud computing.

Mr. Chairman, cloud computing is such an important innovation that it is changing how people, businesses, and government agencies manage information. The Jackson Lee amendment recognizes the importance of cloud computing to our economy, and it is consistent with the objectives of the bill while ensuring that the privacy and civil liberties rights of citizens are protected.

Again, they are doing business with each other. Once we put in the government, the question has to be whether or not the government transmits information that is not necessary. My amendment protects consumers and businesses that are in the midst of providing and helping in their lives to make sure that users have their privacy. The cloud allows users seamless access to information from any location in the United States where the Internet is accessible and available. My amendment protects them and is ready to help clarify this bill, and I ask my colleagues to support this amendment.

Mr. Chair, I yield to the ranking member of the committee, the distinguished gentleman from Maryland.

Mr. RUPPERSBERGER. I just want to thank the gentlelady from Texas for her hard work on this bill, and I support this amendment.

Ms. JACKSON LEE. I reserve the balance of my time.

Mr. ROGERS of Michigan. Mr. Chairman, while I do not oppose this amendment, I ask unanimous consent to control the time in opposition.

The Acting CHAIR (Mr. YODER). Without objection, the gentleman is recognized for 5 minutes.

There was no objection.

Mr. ROGERS of Michigan. I want to thank the gentlelady for working with us. It is her concern and a genuine concern, and we've had discussions on this bill about the protection of privacy. It's an important element of the way we move forward to try to protect those companies that you talk about in the networks that protect the jobs of every American and the privacy of every American.

Every piece of this bill is voluntary. No one is pressured or compelled to give anything to the government under this bill. In fact, the bill contains two important protections to drive this point home:

First, the bill prohibits the government from requiring a private sector entity to share information with the government. It is completely, 100 percent voluntary;

Second, the bill prohibits the government from conditioning the sharing of classified cyber threat intelligence with a private sector entity on the provision of cyber threat information back to the government in return. In other words, no quid pro quo, and this is a good protection that I know the gentlelady supports.

I believe that these important provisions make it very clear that every molecule of this bill is 100 percent voluntary, and this amendment, I think, reaffirms the strong language that is in the bill in order to give that next level of confidence on all the privacy amendments we've adopted today and to make it very clear that it is paramount that we protect individuals' privacy in the conduct of sharing cyber threat information.

I, therefore, support the amendment, and would urge the body to do the

same. Again, I thank the gentlelady for her work on this issue and for working with the committee to come to a better place.

With that, I yield back the balance of my time.

The Acting CHAIR. The gentlewoman from Texas has 45 seconds remaining.

Ms. JACKSON LEE. Again, I say that the cloud is saving consumers and businesses from the loss of valuable data. The Jackson Lee amendment adds to the firewall of protecting Americans' privacy and, in the flow and the discourse of business, of protecting the privacy of our businesses that do not have data that is necessary for the government's information. That should be said over and over again.

I thank both the ranking member and the chairman for their kind remarks, and I ask my colleagues to support the Jackson Lee amendment that provides, again, the firewall of privacy.

With that, Mr. Chairman, I ask support of my amendment, and I yield back the balance of my time.

Mr. Chairman, I want to thank Chairman ROGERS and Ranking Member RUPPERSBERGER for the work in crafting this legislation and the Rules Committee for making my amendment in order.

Mr. Chairman, my amendment is straightforward. It improves the bill by providing that:

Nothing in this Act or the amendments made by this Act shall be construed to provide authority to a department or agency of the Federal Government to require a cybersecurity provider that has contracted with the Federal Government to provide information services to provide information about cybersecurity incidents that do not pose a threat to the Federal Government's information.

Mr. Chairman, the Jackson Lee amendment makes clear that the only instance in which a cloud service provider can share information about a cyber incident with a government agency is when the objective of an attempted intrusion of the service provider's network was to gain unauthorized access to the government's information.

Mr. Chairman, I am pleased to state that this commonsense amendment is supported by interested groups across the spectrum, from the ACLU on the left to the Constitutional Alliance on the right.

In other words, if a cyber incident does not threaten the government's information, then the incident is none of the government's business.

And this is especially true where disclosure to the government would compromise individuals' privacy and proprietary information of businesses.

Mr. Chairman, today something commonly called "the Cloud" plays an unseen but critical part in the lives of millions of Americans and thousands of businesses. Persons and businesses who use iPhones or use Gmail, Yahoo and MSN e-mail services are connected to the Cloud.

Cloud services include popular online services like Facebook, YouTube, "LinkedIn" (a professional networking service) and "Flickr" (a place where millions of personal and family photos are stored).

The Cloud is saving consumers and businesses from the loss of valuable data through storage services like the popular Apple iCloud. The Cloud protects digital information from loss should their computer or smart phone be damaged, lost or stolen. The Cloud also allows users seamless access to information from any location in the United States where internet access is available.

Mr. Chairman, "cloud computing" is such an important innovation that it is changing how people, businesses, and government agencies manage information.

The Jackson Lee amendment recognizes the importance of "cloud computing" to our economy and is consistent with the objectives of the bill while assuring that privacy and civil liberty rights of citizens are protected.

This is an important amendment, and I urge my colleagues to support it.

ORGANIZATIONS ENDORSING JACKSON LEE AMENDMENT

ACLU
Constitutional Alliance
Stop Real ID Coalition
The Constitution Project
The Liberty Coalition

□ 1110

The Acting CHAIR. The question is on the amendment offered by the gentlewoman from Texas (Ms. JACKSON LEE).

The amendment was agreed to.

AMENDMENT OFFERED BY MR. MCCAUL

The Acting CHAIR. It is now in order to consider the amendment printed in section 3 of House Resolution 164 as modified by the order of the House of today.

Mr. MCCAUL. Mr. Chairman, I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

After section 1, insert the following new section (and renumber subsequent sections accordingly):

**"SEC. 2. FEDERAL GOVERNMENT COORDINATION WITH RESPECT TO CYBERSECURITY.**

"(a) COORDINATED ACTIVITIES.—The Federal Government shall conduct cybersecurity activities to provide shared situational awareness that enables integrated operational actions to protect, prevent, mitigate, respond to, and recover from cyber incidents.

"(b) COORDINATED INFORMATION SHARING.—

"(1) DESIGNATION OF COORDINATING ENTITY FOR CYBER THREAT INFORMATION.—The President shall designate an entity within the Department of Homeland Security as the civilian Federal entity to receive cyber threat information that is shared by a cybersecurity provider or self-protected entity in accordance with section 1104(b) of the National Security Act of 1947, as added by section 3(a) of this Act, except as provided in paragraph (2) and subject to the procedures established under paragraph (4).

"(2) DESIGNATION OF A COORDINATING ENTITY FOR CYBERSECURITY CRIMES.—The President shall designate an entity within the Department of Justice as the civilian Federal entity to receive cyber threat information related to cybersecurity crimes that is shared by a cybersecurity provider or self-protected entity in accordance with section 1104(b) of the National Security Act of 1947, as added by section 3(a) of this Act, subject to the procedures under paragraph (4).

"(3) SHARING BY COORDINATING ENTITIES.—The entities designated under paragraphs (1) and (2) shall share cyber threat information shared with such entities in accordance with section 1104(b) of the National Security Act of 1947, as added by section 3(a) of this Act, consistent with the procedures established under paragraphs (4) and (5).

"(4) PROCEDURES.—Each department or agency of the Federal Government receiving cyber threat information shared in accordance with section 1104(b) of the National Security Act of 1947, as added by section 3(a) of this Act, shall establish procedures to—

"(A) ensure that cyber threat information shared with departments or agencies of the Federal Government in accordance with such section 1104(b) is also shared with appropriate departments and agencies of the Federal Government with a national security mission in real time;

"(B) ensure the distribution to other departments and agencies of the Federal Government of cyber threat information in real time; and

"(C) facilitate information sharing, interaction, and collaboration among and between the Federal Government; State, local, tribal, and territorial governments; and cybersecurity providers and self-protected entities.

"(5) PRIVACY AND CIVIL LIBERTIES.—

"(A) POLICIES AND PROCEDURES.—The Secretary of Homeland Security, the Attorney General, the Director of National Intelligence, and the Secretary of Defense shall jointly establish and periodically review policies and procedures governing the receipt, retention, use, and disclosure of nonpublicly available cyber threat information shared with the Federal Government in accordance with section 1104(b) of the National Security Act of 1947, as added by section 3(a) of this Act. Such policies and procedures shall, consistent with the need to protect systems and networks from cyber threats and mitigate cyber threats in a timely manner—

"(i) minimize the impact on privacy and civil liberties;

"(ii) reasonably limit the receipt, retention, use, and disclosure of cyber threat information associated with specific persons that is not necessary to protect systems or networks from cyber threats or mitigate cyber threats in a timely manner;

"(iii) include requirements to safeguard non-publicly available cyber threat information that may be used to identify specific persons from unauthorized access or acquisition;

"(iv) protect the confidentiality of cyber threat information associated with specific persons to the greatest extent practicable; and

"(v) not delay or impede the flow of cyber threat information necessary to defend against or mitigate a cyber threat.

"(B) SUBMISSION TO CONGRESS.—The Secretary of Homeland Security, the Attorney General, the Director of National Intelligence, and the Secretary of Defense shall, consistent with the need to protect sources and methods, jointly submit to Congress the policies and procedures required under subparagraph (A) and any updates to such policies and procedures.

"(C) IMPLEMENTATION.—The head of each department or agency of the Federal Government receiving cyber threat information shared with the Federal Government under such section 1104(b) shall—

"(i) implement the policies and procedures established under subparagraph (A); and

"(ii) promptly notify the Secretary of Homeland Security, the Attorney General, the Director of National Intelligence, the Secretary of Defense, and the appropriate congressional committees of any significant violations of such policies and procedures.

''(D) OVERSIGHT.—The Secretary of Homeland Security, the Attorney General, the Director of National Intelligence, and the Secretary of Defense shall jointly establish a program to monitor and oversee compliance with the policies and procedures established under subparagraph (A).

''(6) INFORMATION SHARING RELATIONSHIPS.—Nothing in this section shall be construed to—

''(A) alter existing agreements or prohibit new agreements with respect to the sharing of cyber threat information between the Department of Defense and an entity that is part of the defense industrial base;

''(B) alter existing information-sharing relationships between a cybersecurity provider, protected entity, or self-protected entity and the Federal Government;

''(C) prohibit the sharing of cyber threat information directly with a department or agency of the Federal Government for criminal investigative purposes related to crimes described in section 1104(c)(1) of the National Security Act of 1947, as added by section 3(a) of this Act; or

''(D) alter existing agreements or prohibit new agreements with respect to the sharing of cyber threat information between the Department of Treasury and an entity that is part of the financial services sector.

''(7) TECHNICAL ASSISTANCE.—

''(A) DISCUSSIONS AND ASSISTANCE.—Nothing in this section shall be construed to prohibit any department or agency of the Federal Government from engaging in formal or informal technical discussion regarding cyber threat information with a cybersecurity provider or self-protected entity or from providing technical assistance to address vulnerabilities or mitigate threats at the request of such a provider or such an entity.

''(B) COORDINATION.—Any department or agency of the Federal Government engaging in an activity referred to in subparagraph (A) shall coordinate such activity with the entity of the Department of Homeland Security designated under paragraph (1) and share all significant information resulting from such activity with such entity and all other appropriate departments and agencies of the Federal Government.

''(C) SHARING BY DESIGNATED ENTITY.—Consistent with the policies and procedures established under paragraph (5), the entity of the Department of Homeland Security designated under paragraph (1) shall share with all appropriate departments and agencies of the Federal Government all significant information resulting from—

''(i) formal or informal technical discussions between such entity of the Department of Homeland Security and a cybersecurity provider or self-protected entity about cyber threat information; or

''(ii) any technical assistance such entity of the Department of Homeland Security provides to such cybersecurity provider or such self-protected entity to address vulnerabilities or mitigate threats.

''(c) REPORTS ON INFORMATION SHARING.—

''(1) INSPECTOR GENERAL OF THE DEPARTMENT OF HOMELAND SECURITY REPORT.—The Inspector General of the Department of Homeland Security, in consultation with the Inspector General of the Department of Justice, the Inspector General of the Intelligence Community, the Inspector General of the Department of Defense, and the Privacy and Civil Liberties Oversight Board, shall annually submit to the appropriate congressional committees a report containing a review of the use of information shared with the Federal Government under subsection (b) of section 1104 of the National Security Act of 1947, as added by section 3(a) of this Act, including—

''(A) a review of the use by the Federal Government of such information for a purpose other than a cybersecurity purpose;

''(B) a review of the type of information shared with the Federal Government under such subsection;

''(C) a review of the actions taken by the Federal Government based on such information;

''(D) appropriate metrics to determine the impact of the sharing of such information with the Federal Government on privacy and civil liberties, if any;

''(E) a list of the departments or agencies receiving such information;

''(F) a review of the sharing of such information within the Federal Government to identify inappropriate stovepiping of shared information; and

''(G) any recommendations of the Inspector General of the Department of Homeland Security for improvements or modifications to the authorities under such section.

''(2) PRIVACY AND CIVIL LIBERTIES OFFICERS REPORT.—The Officer for Civil Rights and Civil Liberties of the Department of Homeland Security, in consultation with the Privacy and Civil Liberties Oversight Board, the Inspector General of the Intelligence Community, and the senior privacy and civil liberties officer of each department or agency of the Federal Government that receives cyber threat information shared with the Federal Government under such subsection (b), shall annually and jointly submit to Congress a report assessing the privacy and civil liberties impact of the activities conducted by the Federal Government under such section 1104. Such report shall include any recommendations the Civil Liberties Protection Officer and Chief Privacy and Civil Liberties Officer consider appropriate to minimize or mitigate the privacy and civil liberties impact of the sharing of cyber threat information under such section 1104.

''(3) FORM.—Each report required under paragraph (1) or (2) shall be submitted in unclassified form, but may include a classified annex.

''(d) DEFINITIONS.—In this section:

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

''(A) the Committee on Homeland Security, the Committee on the Judiciary, the Permanent Select Committee on Intelligence, and the Committee on Armed Services of the House of Representatives; and

''(B) the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Select Committee on Intelligence, and the Committee on Armed Services of the Senate.

''(2) CYBER THREAT INFORMATION, CYBER THREAT INTELLIGENCE, CYBERSECURITY CRIMES, CYBERSECURITY PROVIDER, CYBERSECURITY PURPOSE, AND SELF-PROTECTED ENTITY.—The terms 'cyber threat information', 'cyber threat intelligence', 'cybersecurity crimes', 'cybersecurity provider', 'cybersecurity purpose', and 'self-protected entity' have the meaning given those terms in section 1104 of the National Security Act of 1947, as added by section 3(a) of this Act.

''(3) INTELLIGENCE COMMUNITY.—The term intelligence community' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

''(4) SHARED SITUATIONAL AWARENESS.—The term 'shared situational awareness' means an environment where cyber threat information is shared in real time between all designated Federal cyber operations centers to provide actionable information about all known cyber threats.''.

Page 4, line 18, strike ''Federal Government'' and insert ''entities of the Department of Homeland Security and the Department of Justice designated under paragraphs (1) and (2) of section 2(b) of the Cyber Intelligence Sharing and Protection Act''.

Page 5, line 5, strike ''Federal Government'' and insert ''entities of the Department of Homeland Security and the Department of Justice designated under paragraphs (1) and (2) of section 2(b) of the Cyber Intelligence Sharing and Protection Act''.

Page 5, strike line 6 and all that follows through page 6, line 7.

Page 7, beginning on line 17, strike ''by the department or agency of the Federal Government receiving such cyber threat information''.

Page 13, strike line 13 and all that follows through page 15, line 23.

Page 17, strike line 15 and all that follows through page 19, line 19.

The Acting CHAIR. Pursuant to House Resolution 164, the gentleman from Texas (Mr. MCCAUL) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Texas.

Mr. MCCAUL. Mr. Chairman, I yield myself such time as I may consume, and I want to first thank Mr. ROGERS, Mr. RUPPERSBERGER, Mr. THOMPSON, and all the staff for their real-time collaboration over the last several days, very late night hours, to get this amendment to perfection, and let me just say thanks again for that.

Mr. Chairman, I strongly encourage support of this amendment. Cyber threats that the United States faces are real and immediate, and the key to addressing these cracks in our cyber defenses lies with bridging the gap between government and industry. My amendment helps do just that.

This amendment would direct the Federal Government to conduct cybersecurity activities in a real-time, coordinated, and integrated way so that there is shared situational awareness across agencies to protect the Nation from cyber attack. This amendment would designate an entity within the Department of Homeland Security as the civilian Federal entity interface to receive cyber threat information from the private sector. This is an important improvement and provides an additional layer of review for information sharing procedures by a robust civilian privacy office in order to ensure Americans' civil liberties are protected.

Additionally, another important improvement to the underlying bill by way of this amendment is designating an entity within the Department of Justice as the civilian Federal entity to receive cyber threat information from the private sector related to cyber crime.

This bipartisan amendment improves the underlying bill and addresses concerns raised by privacy groups. These changes ensure that DHS and DOJ will serve as points of entry for those seeking to share cyber threat information with the Federal Government.

With that, Mr. Chairman, I reserve the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Chairman, while I am not opposed to the amendment, I ask unanimous consent to claim the time in opposition.

The Acting CHAIR. Without objection, the gentleman is recognized for 5 minutes.

There was no objection.

Mr. THOMPSON of Mississippi. Mr. Chair, I rise in strong support of this amendment.

Enhancing our security in cyberspace is of the highest importance, but it cannot be done at the expense of our privacy and civil liberties. The key to ensuring the necessary protections are in place is codifying in statute a strong civilian lead for information sharing with the private sector. Our amendment does just that.

Yesterday, I reached an agreement with Chairman ROGERS, Ranking Member RUPPERSBERGER, and Chairman MCCAUL to offer this bipartisan amendment to strengthen the bill. The amendment establishes a center within the Department of Homeland Security as the Federal hub for cyber threat information shared under this bill, and the Department of Justice as the hub for all cyber crime information.

With this amendment, citizens may take comfort knowing that their information will be more likely shared with the appropriate civilian agencies with the accompanying accountability and transparency; and businesses can be more sure that their dealings abroad will not be colored by the perception, fair or otherwise, that they are in cahoots with the National Security Agency.

To be clear, this amendment does not fix all of the privacy or liability issues with the underlying bill, but it does establish the strong precedent of civilian control of cyber information sharing; and I hope we can fix the broader issues with the bill, should it pass, further down the line.

This amendment is absolutely essential to the bill, and it sends the right message to the world about the way the United States will act in cyberspace.

I reserve the balance of my time.

ENHANCE THE CIVILIAN AUTHORITIES IN CISPA

ENHANCE THE CIVILIAN AUTHORITIES IN CISPA

DEAR COLLEAGUE: Chairman Rogers and Ranking Member Ruppersberger of the House Permanent Select Committee on Intelligence, together with Chairman McCaul and Ranking Member Thompson of the House Homeland Security Committee, will offer an amendment that will designate a civilian lead for the cyber security information sharing program under the Cyber Intelligence Sharing and Protection Act (CISPA).

This amendment requires the President to designate a civilian entity within the Department of Homeland Security (DHS) to be the entry point to receive cyber threat information and to designate an entity within the Department of Justice (DOJ) as the civilian entity to receive cyber threat information related to cybersecurity crimes. These changes make clear that DHS and the DOJ will serve as points of entry for those seeking to share cybersecurity threat information with the federal government.

The amendment also requires the Secretary of DHS, the Attorney General, the Director of National Intelligence, and the Secretary of Defense to establish procedures to eliminate any personal information from cyber threat information shared with the federal government. Cyber threat information shared with the government from any source will be scrubbed of any personally identifiable information and deleted—this is also known as ''minimization.''

Every agency receiving cyber threat information must notify these four agencies, and Congress of significant violations of the procedures required by the bill. These agencies must also establish a program to oversee compliance with the minimization procedures.

We urge you to vote ''yes'' on this amendment.

Sincerely,

MICHAEL T. MCCAUL,
*Chairman, Homeland Security Committee.*

BENNIE THOMPSON,
*Ranking Member, Homeland Security Committee.*

MIKE J. ROGERS,
*Chairman, Permanent Select Committee on Intelligence.*

DUTCH RUPPERSBERGER,
*Ranking Member, Permanent Select Committee on Intelligence.*

Mr. MCCAUL. Mr. Chairman, I yield such time as he may consume to the distinguished gentleman from Michigan (Mr. ROGERS), the chairman of the Permanent Select Committee on Intelligence.

Mr. ROGERS of Michigan. Mr. Chair, I want to thank Mr. THOMPSON and Mr. MCCAUL for working so hard on this particular amendment to try and get it right. An agreement was agreed to and then undone, and then agreed to by some involvement who are filled with self-importance beyond this Chamber. We were able to work out those differences and get to a place where we all agreed.

This is an important amendment. This is that civilian face that so many talked about for so long on this bill. And I want to thank both the chair and the ranking member of Homeland Security for working through all of the difficulties to get us to this place where we could present that civilian face and add yet one more reassurance about privacy, civilian liberty protection, and that this is not a surveillance bill.

And I want to thank again Mr. THOMPSON for your graciousness, your patience for working with us, and Mr. MCCAUL for your leadership on this issue as well. I urge strong support for the McCaul-Thompson-Ruppersberger-Rogers amendment.

Mr. THOMPSON of Mississippi. Mr. Chairman, I yield 1 minute to the gentlewoman from California (Ms. PELOSI), the distinguished Democratic leader.

Ms. PELOSI. Mr. Chairman, today the Internet and new technologies are shaping a world that we could scarcely have imagined even 10 years ago. It's giving Americans an easy way to build friendships, build business, and participate in democracy, all with the click of a button.

But because so much of our daily lives are invested in cyberspace, it only takes one more click to put our personal identities, our economic stability, and our national security at risk. The threat of a cyber attack on our country is real, and our response must always balance our security with our liberties. That has always been the case in the history of America, the balance between liberty and security.

There can be absolutely no doubt or delay in shoring up our Nation's cybersecurity. We must take clear, responsible, effective action to enhance the security of the American people.

I want to commend Chairman ROGERS and Ranking Member RUPPERSBERGER, working together in a bipartisan way, for their leadership on this issue and their efforts to craft and try to improve this legislation. I want to thank Chairman MCCAUL and Ranking Member THOMPSON on the Homeland Security Committee for their energetic leadership on this subject as well. I thank both committees for recognizing the jurisdiction of the other committee.

I had hoped that today we would be addressing some major concerns of Members of Congress and the White House by improving the legislation's protections of personal information. With all of the respect in the world for the work of our chairs and ranking members on this, and it has been considerable. You have standing on this issue that is recognized and respected. I am disappointed, however, that we did not address some of the concerns, as I mentioned, of the White House about personal information.

Unfortunately, this bill offers no policies, did not allow any amendments—and I don't put that to you, no amendments—and no real solutions that adequately uphold an American's right to privacy.

For one thing, in promoting the sharing of cyber threat information, the bill does not require the private sector to minimize irrelevant personally identifiable information from what it shares with the government, or other private matters. They can just ship the whole kit and caboodle. We are saying minimize what is relevant to our national security; the rest is none of the government's business.

The bill continues to offer overly broad liability protections and immunities to the businesses that could violate our liberties rather than offering more targeted liabilities to ensure that the private sector only shares appropriate information.

□ 1120

We thought there might be a way to get this done by amendment—I'm sure that it would enjoy bipartisan support—but the Rules Committee did not allow that amendment to come forward.

Most importantly, the bill fails to critically address the greatest weakness in our cybersecurity: our Nation's infrastructure. Too many of our country's systems, both physical and virtual, are still exposed to an increasing number of intrusions and attacks.

Now, as a longtime former member of the Intelligence Committee, I know that infrastructure is not your jurisdiction, so in your original bill you couldn't go to that place. But now the Rules Committee could have allowed, with the cooperation of the Homeland Security Committee, us to go into infrastructure.

If we're truly going to secure a reliable and resilient cyberspace that reflects our country's values, we must target our clearest vulnerabilities, while preserving a space that promotes the innovation, expression, and security of the American people.

The world we live in and the threats our country faces can change with just one click. While we should never let Americans doubt our vigilance, our preparation, our effectiveness, we must never let us compromise their civil liberties.

If we fail to meet the standard of security, we always do more harm than good.

I, myself, am personally going to vote ''no'' on this legislation but, in doing so, salute the chairs and ranking members of the committees for taking us way down the road on this issue. It's just that crucial balance between security and liberty that I do not think has been struck in that bill. So, for my own part, it will not have my support.

Mr. MCCAUL. We have no more speakers. I reserve the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Chair, I yield 1 minute to the gentleman from Maryland (Mr. RUPPERSBERGER), the ranking member on the Committee on Intelligence.

Mr. RUPPERSBERGER. First thing, I want to thank the ranking member, Mr. THOMPSON, and I want to thank Mr. MCCAUL and Mr. ROGERS for coming together. That's what we're elected to do, to come together in a bipartisan way and to deal with difficult issues. And they were difficult issues. But we're here today to all support this amendment.

The White House and the privacy groups raised this as one of the main issues with the bill. These groups were concerned that there was an impression, wrongly, I believe, that the military would control the program. This was never the case, but we heard these concerns, and we are addressing them in this amendment.

It means that companies sharing information about cyber threats will go to the Department of Homeland Security, a civilian agency. If the information is related to cybersecurity crime, the companies will go to the Department of Justice, another civilian agency.

The amendment requires that the Department of Homeland Security share this information with other government agencies in real-time so they can use it to protect against future cyber threats and attacks.

This amendment ensures we protect the security of our Nation, but also protect the privacy and liberties of our country and our citizens. I strongly support this amendment and urge other Members to do the same.

I commend, again, Ranking Member THOMPSON, Chairman MCCAUL, Chairman ROGERS for coming together at the last moment. I respectfully request a ''yes'' vote on the amendment.

You can't have security if you don't have privacy and liberty.

Mr. THOMPSON of Mississippi. Mr. Chair, who has the right to close?

The Acting CHAIR. The gentleman from Mississippi has the right to close.

Mr. THOMPSON of Mississippi. I reserve the balance of my time.

Mr. MCCAUL. Mr. Chairman, I yield myself the balance of my time.

Let me just say this: when it comes to this issue, particularly, which we know is one of the greatest threats that the United States faces right now, and that's the threat of cyber attacks, this is not a Republican-Democrat issue. It's really an American issue.

And with all due respect, this does provide, I think, the balance between security and civil liberties; and it provides the civilian interface to the private sector to protect our critical infrastructures that are already under attack by countries like Iran, China, and Russia.

So I think that, if anything, the recent events in Boston demonstrate that we have to come together as Republicans and Democrats to get this done in the name of national security. In the case in Boston, they were real bombs, explosive devices. In this case, they're digital bombs, and these digital bombs are on their way.

That's why this legislation is so important. That's why it's so urgent that we pass this today. For if we don't, and those digital bombs land and attack the United States of America, and Congress fails to act, then Congress has that on its hands.

I yield back the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Chair, at this point, I'd like to say that I agree with Democratic Leader Ms. PELOSI's issue with respect to cyber, particularly critical infrastructure. And I look forward to working with Chairman MCCAUL on submitting legislation.

With that, Mr. Chair, I encourage Members to support this bipartisan amendment that the chair of the Committee on Homeland Security and I drafted.

I yield back the balance of my time.

Ms. JACKSON LEE. Mr. Chair, I am in support of the amendment offered by Intelligence Committee Chairman ROGERS, Congressman MCCAUL and Homeland Security Ranking Member THOMPSON to H.R. 624, the Cyber Intelligence Sharing and Protection Act of 2013. This is very similar to the amendment I offered before the Rules Committee, but was not made in order. I am pleased that the focus of my amendment is addressed by this amendment that was made in order.

This amendment just as I outlined in my amendment offered to the Rules Committee would establish a lead role for the Department of Homeland Security—a civilian agency in matters related to cyber security threats. DHS would be the agency to receive all cyber threat information. This amendment designates the Department of Justice (DOJ) as the civilian entity to receive cyber threat information related to cybersecurity crimes.

These changes make clear that DHS and the DOJ will serve as points of entry for those seeking to share cybersecurity threat information with the federal government.

The amendment also requires the Secretary of DHS, the Attorney General, the Director of National Intelligence, and the Secretary of Defense to establish procedures to eliminate any personal information from cyber threat information shared with the federal government. Cyber threat information shared with the government from any source will be scrubbed of any personally identifiable information and deleted—this is also known as "minimization."

Every agency receiving cyber threat information must notify these four agencies, and Congress of significant violations of the procedures required by the bill. These agencies must also establish a program to oversee compliance with the minimization procedures.

The importance of a civil agency in a central role regarding the establishment and functions of domestic cyber protection programs is critical to building in the transparency, accountability and oversight the American public expects. I am in strong support of this amendment and thank my colleagues for their efforts to address the concerns of many of our constituents as we work to assure the Internet is as safe as it can be and that we maintain the level of oversight that is needed.

This is an important amendment, and I urge my colleagues to support it.

The Acting CHAIR. The question is on the amendment offered by the gentleman from Texas (Mr. MCCAUL).

The question was taken; and the Acting Chair announced that the ayes appeared to have it.

Mr. MCCAUL. Mr. Chairman, I demand a recorded vote.

The Acting CHAIR. Pursuant to clause 6 of rule XVIII, further proceedings on the amendment offered by the gentleman from Texas will be postponed.

Mr. ROGERS of Michigan. Mr. Chairman, I move that the Committee do now rise.

The motion was agreed to.

Accordingly, the Committee rose; and the Speaker pro tempore (Mr. DENHAM) having assumed the chair, Mr. YODER, Acting Chair of the Committee of the Whole House on the state of the Union, reported that that Committee, having had under consideration the bill (H.R. 624) to provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, and for other purposes, had come to no resolution thereon.

## RECESS

The SPEAKER pro tempore. Pursuant to clause 12(a) of rule I, the Chair declares the House in recess subject to the call of the Chair.