NOT VOTING—13

Bachmann	Kennedy	Rangel
Blackburn	Lynch	Shimkus
Gohmert	Markey	Westmoreland
Holding	Miller, Gary	
Hurt	Neal	

□ 1418

Mr. RAHALL, Ms. PELOSI, Ms. BROWNLEY of California, Mr. CÁRDENAS and Ms. WILSON of Florida changed their vote from ''yea'' to ''nay.''

Messrs. KING of New York, YOHO and AMASH changed their vote from ''nay'' to ''yea.''

So the resolution was agreed to.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

APPOINTMENT OF MEMBERS TO THE BOARD OF VISITORS TO THE UNITED STATES COAST GUARD ACADEMY

The SPEAKER pro tempore (Mr. RODNEY DAVIS of Illinois). The Chair announces the Speaker's appointment, pursuant to 14 U.S.C. 194, and the order of the House of January 3, 2013, of the following Members on the part of the House to the Board of Visitors to the United States Coast Guard Academy:

Mr. COBLE, North Carolina

Mr. COURTNEY, Connecticut

□ 1420

CYBER INTELLIGENCE SHARING AND PROTECTION ACT

GENERAL LEAVE

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

The SPEAKER pro tempore. 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 consideration of the bill, H.R. 624.

The Chair appoints the gentlewoman from Florida (Ms. ROS-LEHTINEN) to preside over the Committee of the Whole.

□ 1422

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 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 Ms. ROS-LEHTINEN in the chair.

The Clerk read the title of the bill.

The CHAIR. Pursuant to the rule, the bill is considered read the first time.

The gentleman from Michigan (Mr. ROGERS) and the gentleman from Maryland (Mr. RUPPERSBERGER) each will control 30 minutes.

The Chair recognizes the gentleman from Michigan.

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

I want to thank my ranking member and both the Republican and Democratic staffs and the Republican and Democratic members of the Intelligence Committee for 2 years of long hours in negotiated efforts to reach the point that we are.

I want to back up just a little bit and tell you how we got to where we are today. We sat down some 2 years ago when the ranking member and I assumed the leadership of the Intelligence Committee and we looked at the one threat that we knew existed but we were not prepared to handle as Americans, both the private sector and the government. And we knew that we had to do something about this new and growing and misunderstood cyber threat and what it was doing to our intellectual property across the country, what it was doing to the freedom and open Internet that we so enjoy and are increasingly dependent on and the commercial value of our growing economy. And it was at risk. The private sector was at risk because people were stealing their identities, their accounts, their intellectual property, and subsequent to that, their jobs, and people began to question the value of getting on the Internet and using it for commercial purposes. Their trust in the free and open Internet the way we've embraced it in the United States really was at risk.

How do we solve that problem? We knew that nation states were investing millions and billions of dollars to generate cyber warriors to go in and crack your computer network. I don't care if you had intellectual property—those blueprints that made your business successful, or maybe it was your bank account, or your ability to have a transaction. If they could interrupt that, they could do great harm to our economy and to the United States.

We saw nation-states like Russia and China and now Iran and North Korea and others developing military-style attacks to actually do harm to the U.S. economy, to hurt the very men and women who get up every day and play by the rules and think that the Internet would be a safe place for them to interact when it comes to commerce. We want that to continue.

So we sat down and we talked to industry folks, people who are in the business, high-tech industry folks from Silicon Valley, financial services folks from New York City, manufacturers from across the Midwest, who were losing intellectual property due to theft from nation-states like China. We talked to privacy groups. We talked to the executive branch. And over the last 2 years, there were some 19 adjustments to this bill on privacy.

We believe this: this bill will not work if Americans don't have confidence that it will protect your privacy and civil liberties while allowing one very simple thing to happen: cyber threat material, that malware that goes on your computer and does bad things, allows somebody else to take over your computer to attack a bank, allows them to go on your computer and steal your personally identifiable information and use it in a crime, allows them to go into your network at work and steal your most valuable company secrets that keep you alive and build great products here in the United States—could we allow the government to share what they know with the private sector and allow the private sector to share when it comes to just that cyber threat, those zeros and ones in a pattern that equates to malicious code traveling at hundreds of millions of times a second the speed of light, can we share that in a way to stop them from getting in and stealing your private information?

And the good news is the answer is, yes, we can do this. We can protect privacy and civil liberties, and we can allow this sharing arrangement, but not of your identity, not of your personally identifiable information. As a matter of fact, if that's what's happening, it won't work. But at the speed of light, from machine to machine, from your Internet service provider before it ever gets into your network they bounce out the nastiest stuff that's in there that's going to take over your computer, steal your money, steal your personally identifiable information, steal your company secrets. And they can identify that by a pattern and kick it out. They'll say, Something looks bad about that. Can the government take a look at that and say, you know what? This is a Chinese attack, it's an Iranian attack, it's a North Korean attack—let's defend our networks. It's really very simple.

Today, what you see is a collaborative effort. This isn't a bill by DUTCH RUPPERSBERGER and MIKE ROGERS and this is the only way it has to be. We have taken suggestions from all the groups I just talked about, from privacy to the executive branch to industry to other trade associations. And this is the bill that mutually all of those people, representing tens of millions of employees around this country, said this is the way you do this and protect the free and open Internet and you protect civil liberties. And you finally raise that big red sign that tells people like China and Iran and Russia, stop. We're going to prevent you from stealing America's prosperity.

I heard a lot of debate earlier on the rule. I've heard a lot of misinformation. There are people who don't like it for whatever reason, maybe it's conviction, maybe it's politics, maybe it's political theater. And I have a feeling there's a little bit of all of that when they talk about this bill.

This bill does none of the things I've heard talked about in the rule—that

it's an exchange of information that they've never seen with the government. This is not a surveillance bill. It does not allow the national security agencies or the Department of Defense or any of our military organizations to monitor our domestic networks. It does not allow that to happen. We would not allow that to happen.

□ 1430

So some notion that that's happening is just wrong, and some of the folks who are pretending otherwise know it's wrong. This is important.

You know, the Iranians, by public report, are laughing at our shores, looking for weaknesses in our financial institutions. They're not doing it for benevolence. They're doing it to try to create chaos in our markets here at home. This isn't 10 years or 20 years. This is today. It's happening today.

The average credit card in your purse, Madam Chair, will be hit 300,000 times today by bad actors trying to get in and steal your personal information—all those cardholders' information—and use it to commit a crime.

Today, hundreds of millions of times across this great country companies will be besieged by DDoS attacks trying to overwhelm their systems and shut them down and not allow commerce to happen, by people who are trying to get into their networks and steal something valuable.

This bill is that right balance between our privacy, civil liberties, and stopping bad guys in their tracks from ruining what is one-sixth of the U.S. economy. It's that important, and it's important that we get at it today.

We must do more to improve our cybersecurity, and this bill is that vital first step toward that bill. Our intelligence agencies collect important information overseas about advanced foreign cyber threats that could dramatically assist the private sector. That information is the intelligence community's unique value-added when it comes to our cybersecurity.

Unfortunately, we are not getting the full value of those intelligence insights. As I said, the intelligence community is not monitoring the Internet. They don't know what's happening on the domestic Internet. So when there is a nasty piece of source code or malicious source code attacking the private sector, the only way we're going to know that is if we—and these folks are victims of crime, by the way—if we allow them, in a classified environment, to share malicious source codes—zeros and ones in the right pattern—with the government and say, Hey, I am the victim of a crime. Here's what it looks like. Can you help? The government needs to be able to share this threat intelligence so that the private sector can protect its own networks.

The government is going to reciprocate. Our intelligence services go overseas. They find out what the bad guys are doing. They come back and protect the government networks. The problem is, because of laws and policies and procedures, we can't share that with the private sector so they can protect their own networks. Wouldn't it be great if they know what's coming? If you know what you're looking for, you can stop it. That's really what we're talking about doing here, Madam Chair.

We must also modernize the law to give the private sector clear authority to share cyber threat information within the private sector, as well as the government, on a voluntary, anonymous basis.

Again, if you believe in the free and open Internet and you look at all the bills that have been introduced, there is a chomping at the bit in this town to go out and try to put their mitts on the Internet. They want to get in there and start regulating and standards and setting up procedures. They want to get in from business-to-business communication. They want the government to be at every corner of the Internet. I reject that wholly. It's the wrong approach. It will not work. It will bring the Internet to a halt. This is the only bill that doesn't have new mandates, new authorizations for any government involvement in the Internet.

It does something very simple. I'm going to repeat it a lot today, Madam Chair. It allows the government to share zeros and ones in the right pattern with the private sector. And zeros and ones from the private sector, when they know it's malicious and attacking their networks, they share it with the government and say, This is a problem. Can you help me? That's what this bill does. And we've got a long list of privacy protections and restrictions to make sure that that's all that this bill does. The bill achieves all of these important goals that I just walked through, and it will empower the private sector, which already does significant work to protect computer networks, to do even more.

The bill will allow the government to share cyber threat intelligence more widely with American companies in operationally usable form so they can help prevent state-sponsored cyber spies from stealing American trade secrets. It also provides clear, positive authority to allow companies to share cyber threat information with others in the private sector. It also provides authority to allow those companies to share threat information on a purely voluntary and anonymized basis with the government, meaning no personal identifying information.

This bill will not require additional Federal spending. It will not require the creation of a vast new government bureaucracy. It will not impose any Federal regulations or unfunded mandates on the private sector. To the contrary, it will be a critical, bipartisan first step toward enabling America's private sector to better defend itself from the advanced state-sponsored cyber threats in which we live in today.

I'm very proud of the open and transparent process that produced this bill. We've had a great conversation over the last 2 years with a broad range of private sector companies, trade groups, privacy and civil liberties advocates, and the executive branch. I appreciate all the constructive input we have received from the process. This bill has been revised every step of the way in this process, and all of that has been based on discussions with all the groups I just mentioned.

I just want to cover some of the privacy protections we've added along the way.

The bill prohibits the government from requiring private sector entities to provide information to the government. There is nothing in here that has any requirement that the private sector must share cyber threat information. If they don't think it's in their best interest to stop that cyber crime, they don't have to say a word. If they do, they're allowed to share just that cyber threat information with the right agencies in real time. Again, this is machine to machine so that they can deal with the international nature of that threat.

It encourages the private sector to anonymize or minimize the information it voluntarily shares with others, including the government.

In addition, the bill requires an annual independent inspector general audit and report to Congress of all voluntary information sharing with the government. That's another layer of oversight. We have built multiple layers of oversight into this bill so that we can gain the confidence of the public in its purpose, intent, and success.

The bill significantly limits the Federal Government's use of information voluntarily provided by the private sector, including a restriction on the government's ability to search that data—very important.

The bill also enforces the restrictions on the government by levying penalties against the government through Federal court lawsuits for any violations of those restrictions. Again, another layer of oversight.

In the markup, we've made some progress, as well, between the ranking member and the members on the committee negotiating and working out what changes we can make to, again, improve the confidence that people have in this bill. We have improved this bill every step of the way for the last 2 years, and the markup was no different. At our markup, which voted the bill out of committee on a strong 18–2 vote, we adopted five important amendments to further strengthen the bill's protections and safeguards.

We adopted an amendment by Mr. LANGEVIN that made it clear that the bill contained no new authority to allow companies to hack back into networks in other companies. It certainly wasn't intended in the legislation. I thought it was a well-intended amendment. The last thing we want to do is

unleash digital vigilantism across the country and what that might do to our ability to continue to rely on the Internet as an engine of commerce.

We've put in place the private sector use restriction that limits companies' use of information received to only cybersecurity purposes. Mr. HECK and Mr. HIMES worked diligently on this amendment to improve the bill and make it very clear that this is just about cybersecurity and cybersecurity purposes.

The bill previously gave the government authorization to create procedures to protect privacy and civil liberties and prevent the government's retention of personal information not necessary to understand a cyber threat. Last week's amendment makes those procedures mandatory. That was by Mr. HIMES. We agreed that was the right place to put the burden to make sure there was no personal identifiable information that was not necessary to determine the nature of the attack.

We also struck the bill's authorized government ''national security'' use of information received from the private sector. This would have provided the government flexibility in the future to address advanced cybersecurity threats. In conversations with government national security lawyers in recent months, they assured us that this flexibility wouldn't be required in the near future. In light of that, and given the widespread misunderstanding this language was generating, we thought it was prudent to take it out. Ms. SEWELL from Alabama offered that amendment and worked with the committee to make sure it was adopted.

We also added additional oversight in the already very strong oversight structure in the bill to monitor the government's receipt and use of cyber threat information voluntarily provided by the private sector. We added roles for the Privacy and Civil Liberties Board and the individual agency privacy officers to provide additional oversight of the government's use of information received from the private sector under this bill.

I'm also very proud to cosponsor an amendment today with Mr. MCCAUL and Mr. THOMPSON of Mississippi, Mr. RUPPERSBERGER and myself that would put a civilian face on the privacy sector cyber information sharing with this government. It was a concern by many. It was something we had long debates and conversations on, and I think we came to an agreement that will at least end that debate. It puts the appropriate civilian face so that, again, people can have confidence in the intention of this bill and what it will do to protect cybersecurity on networks or allow the private sector to protect their own networks and protect civil liberties of Americans.

□ 1440

Other elements of the government, such as the intelligence community, will still receive the information they need to play their important roles, but only after it has been minimized and screened by a civilian entity like the DHS or, in some rare cases, the FBI.

This bill already contains several levels of strong protections to ensure that it improves cybersecurity without compromising our important civil liberties, but this bill will add a significant new privacy protection to that existing structure.

Again, Madam Chair, you can see the level of effort that we are doing here to protect privacy and civil liberties and still have a workable bill that stops nation-states like China, Russia, Iran, and North Korea from getting into your networks and stealing your property.

We have yet to find a single U.S. company that opposes this bill. In fact, we have the enthusiastic support of nearly every sector of the economy, because they are under assault from foreign cyber attacks and they need our help. They need it now. Companies and industry groups from across the country, including Intel, the chip maker, IBM, the Internet Security Alliance, the U.S. Chamber of Commerce, the Business Roundtable, TechAmerica, TechNet, companies of Silicon Valley, the Financial Services Roundtable, U.S. Telecom, the Nuclear Energy Institute, and the National Association of Manufacturers, just to name a few, have sent the committee letters of support. And that list is growing by the day of people who are encouraged by the very light touch of the government; no new programs, no new authorizations, it's not a surveillance bill. This is the only appropriate way to try to deal with this problem.

By allowing the private sector to expand its own cyber defense efforts and to employ classified information to protect systems and networks, this bill will harness private-sector drive and innovation while also keeping the government out of the business of monitoring and guarding private-sector networks.

This important legislation would enable cyber threat sharing and provide clear authority for the private sector to defend its own networks while providing strong protections for privacy and civil liberties.

Madam Chair, with this great collaborative effort, with the effort facing this country, when you see this many Republicans and Democrats coming together, recognizing the threat and crafting a bill that meets that very important standard, this is the bill we should all stand up and enthusiastically support, and I reserve the balance of my time.

Mr. RUPPERSBERGER. Madam Chair, I yield to the gentleman from Illinois (Mr. GUTIERREZ) for the purpose of making a unanimous consent request.

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

Mr. GUTIERREZ. I thank the gentleman for yielding.

Madam Chair, as a member of the House Permanent Select Committee on Intelligence, I am very familiar with the types of threats that this country faces every day and the serious ramifications of cyber vulnerabilities. This is an issue to which the committee has devoted a great deal of time and energy during the last year.

In the cyber security realm these threats are growing in frequency and severity, so much so that the Director of National Intelligence, James Clapper, identified cyber security as a top threat facing this country earlier this year. Director Clapper stated in an open hearing just a month ago that the growing cyber capabilities of both state and non-state actors ''put all sectors of our county at risk, from government and private networks to critical infrastructures.'' We have seen more and more brazen attacks, from financial institutions and banks to news outlets, credit card companies, telecommunications providers and even government entities.

I believe that we should make every effort to safeguard the privacy of Americans' personal information even as we take steps to prevent attacks to our electronic networks and attempts to steal trade secrets, facilitate critical information sharing, and protect our critical infrastructure.

To that end, the committee made a number of improvements to the bill with bipartisan support during our markup last week. Most notably, we voted to remove the authority for private information to be used for broad non-cyber ''national security'' purposes. We also expanded oversight responsibilities for the Privacy and Civil Liberties Oversight Board and restricted usage of information received by private entities to cyber security information. The bill also requires the government to minimize any personal information that is unrelated to a cyber threat. The bill has improved since the last time it was considered by the House of Representatives in 2012.

I understand that there remain areas of concern for some of my colleagues. I share your reservations and am disappointed that we were unable to adopt amendments to address some of the liability issues, require private sector entities to make ''reasonable efforts'' to remove irrelevant personally identifiable information, and establish the Department of Homeland Security as the primary receptor of cyber threat information. An amendment to place DHS as the primary agency was not made in order today and I hope that we can continue to work on an agreement to do that.

I am sensitive to these privacy concerns and hope that we can continue to improve the Cyber Intelligence Sharing and Protection Act through amendments today and ongoing dialogue. However, my underlying concerns about the national security implications of ever-present and even escalating cyber attacks compels me to support the bill today.

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

Chairman ROGERS and I are here today to discuss the Cyber Intelligence Sharing and Protection Act, known as CISPA. The bill simply allows the government to give cyber threat intelligence to the private sector to protect its networks from cyber attacks.

I don't want to repeat a lot of what the chairman has said, but the first

thing I want to do is to acknowledge the leadership of the chairman. Three years ago, the chairman and I, when we took over the leadership of the House Select Intelligence Committee, realized how serious the threat of cyber attacks were to our country, to our businesses, to our health, safety, and welfare.

We decided to pull together a group of representatives from different parts of this issue—we had the administration involved, we had the privacy groups involved, including the ACLU, we brought in the industry—because we knew that we had to put together a bill that would pass the House, the Senate and be signed by the President.

So, what we attempted to do was get input, and then we put together a bill. And, by the way, the bill is only 27 pages—it's probably a record in this Congress—and we did read the bill.

Now, what we attempted to do in this bill is to address a situation where now, the government cannot really communicate with the private sector to try to help protect our citizens, our businesses from cyber attacks. The reason for that is in 1947, there is a law that says that the intelligence community cannot communicate or pass information to another entity that does not have clearances. So, basically what our bill does is to allow the sharing of information, which we can't do now, to the private sector.

Now, why is this important? This is something that is very important because most people don't understand this. In the United States of America we have 10 companies, called the providers, that control 80 percent of our network—80 percent of our network. So in order for us to protect the United States of America from cyber attacks, we need to make sure that the government has a partnership with the private sector and that they can pass the threat information so that the government can help protect.

As an example, if your house is being robbed, you call 911 and the police department comes. That's the same scenario that we're looking at here, only it's a lot more sophisticated. Again, as the chairman said, passing information, mostly zeroes and ones, to the government so that we can work together to protect our network.

Now, why is this so important? And I think it's important that we get into some of the issues of threats. Just recently, we understand, and we know, that The Washington Post, The New York Times, The Wall Street Journal, were cyber-attacked. And basically, our understanding is that they did this, especially China, to intimidate the paper sources within China. We had our U.S. banks. It is very serious for U.S. banks to be attacked and hacked. Most of what our banks have are records and information. And to be able to shut down a bank or to be able to manipulate or get privacy information could be very destructive to our banks, and yet this is being done, and it's been done for a period of time.

Media reports have said that Iran, a rogue country that we know exports terrorism—we know what Iran's beliefs are, and yet reports have said that Iran attacked Saudi Arabia's oil company, one of the largest in the world, Aramco, and wiped out 30,000 computers in a weekend. And let me say this: Iran is not a very sophisticated company as it comes to cyber, but they have the sophistication to be able to knock out 30,000 computers and really shut their businesses down for a period of time. This is what's happening in the United States.

Cyber Command, whose job it is to protect our military networks, estimated that in the last couple of years that we have had, the United States of America has had $400 billion—not million, billion—worth of American trade secrets being stolen from U.S. companies every year, costing these companies market share and jobs. That's probably the biggest theft in the history of the world, and yet we still are not able to help government working with business.

You have Secretary Napolitano, the Director of the FBI, you have the Director of the NSA, Alexander, and all three have said one of the biggest fears they have now are these attacks, and that unless we have a sharing opportunity between government and between business, they feel that they cannot protect our country from these cyber attacks the way that they should. It's so important that we need to act now on this bill.

Now, we can pass bills in the House all day long, but if the Senate doesn't pass a bill and the President doesn't sign it, where are we? We were able to pass our bill last year in a bipartisan manner, and yet our bill went to the Senate and it stalled and the bill didn't go anywhere, so Chairman ROGERS and I started again.

But, what we said to each other and we discussed was that we need to address the issue of privacy. Even though we felt strongly that our bill does protect privacy, we knew there were groups out there, especially the privacy groups, that felt that there was not enough protection in our bill. So we rolled up our sleeves, we listened to the issues raised by the privacy groups, the administration had issues with respect to privacy, and we changed the bill.

Now, I don't want to repeat what the chairman said, but basically we made some significant changes to our bill to deal with the issue of privacy. We provided that first, there's a privacy and civil liberties oversight board, and now that board must review our program. That's one area of oversight.

In the intelligence community, we have privacy officers in each department, in each area. And these privacy people have to look at the threat information. They must also conduct a classified and unclassified review. That's the second oversight that was changed in the bill.

□ 1450

An annual report must be sent to Congress. We also have what we call the ''inspector general,'' whose job it is to oversee the different agencies they represent. Those are four areas of oversight just in the bill.

Regarding the privacy agreements that we were concerned about, we only have five elements where this bill applies. That means if you're a tax cheat and we pick up some information, that can't be used against you. The privacy agreements were concerned about the issue of national security being one of those elements in this bill. They thought it was too broad. So Chairman ROGERS and I got together, and we were able to get the votes from both sides of the aisle, and we were able to take a position that the national security issue is not in the bill anymore. We feel national security is being covered by one of the elements in the bill that says it deals with the issue of protecting people's lives or liberty. So we feel that we have covered national security.

One of the most important issues was the issue of minimization. What is minimization? Most people don't know what it is. Basically, minimization is if private information is passed, there needs to be an entity out there that will take that private information out so that it is not used.

We've now added to the bill that any of the zeroes and ones that are passed—and that's what's happening—if there was some reason why somebody's personal information is passed when those zeroes and ones are coming back and forth, now we have what we call 100 percent minimization, and the government will make sure that every single entity and all the information that is passed will be 100 percent minimized. If there is any personal information in there at all, it will be knocked out. That's very significant, and that gives a lot of coverage.

This is also important: you don't have security if you don't have privacy. That was one of the themes Chairman ROGERS and I used in the beginning: if you don't have security, you don't have privacy. Even though we thought our first bill had it, we felt there was a certain perception, we heard what was said and we made these changes.

There is one other issue that is out there that's very important that I think is also extremely relevant. That's the issue of when the information is passed when we're attempting to protect our citizens and our businesses from these attacks and hopefully from a destructive attack like Iran did to Aramco in Saudi Arabia, there was a perception out there which, again, had to deal with perceptions. The perception was that if this information of zeroes and ones that are being passed back and forth, what is the point of entry. We did not want the perception to be that the military in any way would be in charge or would

be the entity that is overseeing this. We felt very strongly that it had to be civil.

So Chairman ROGERS and I, along with Chairman MCCAUL of the Homeland Security Committee and Ranking Member THOMPSON, have an amendment here today which is very significant. I'm sure it will be very well received by the privacy groups in the White House. What the bill will now say is that when information is passed, it will be the Department of Homeland Security. That is very significant, and we would hope that that would truly deal with the majority of these privacy issues.

We know that we have to move and we have to move quickly. We're here today to debate this bill. And, again, Chairman ROGERS—he's not listening, but I'll say it anyhow—has shown tremendous leadership. I say this and I say it sometimes in jest, that I was a former investigative prosecutor and he was a former FBI agent and all good FBI agents must listen to their prosecutors, even if we're in the minority. That was a joke. Not withstanding that, he has shown leadership. We threw partisanship out the window. We knew the stakes were high. We have been concerned that we have not been able to protect our country. I believe that Congress needs to act because we're standing in the way of protecting our country.

This reminds me of a situation. We know how serious Hurricane Sandy was. It's similar to if you are a meteorologist and Sandy is coming up the east coast and you can't warn your constituents that Sandy is coming. That's why we need to pass this bill tomorrow, and we need to do it for the benefit of our country.

And I do want to end with this: you do not have security if you don't have privacy. We feel that this bill, along with the amendments that will be introduced today, will effect that.

With that, I reserve the balance of my time.

Mr. ROGERS of Michigan. Madam Chair, I yield 3 minutes to a current military officer and great member of the Intelligence Committee, the gentleman from Nevada (Mr. HECK).

Mr. HECK of Nevada. I want to begin by thanking both the chairman and the ranking member for their incredible leadership on this very difficult task. It was especially gratifying to work in such a bipartisan manner to come to the final product that we'll be voting on later tomorrow.

Madam Chair, our Nation is under attack every day, every hour, every minute. Cyber attacks on our Nation's networks threaten our economic and national security. That is why I rise in support of H.R. 624, the Cyber Intelligence Sharing and Protection Act.

Whether it is hacktivists attempting to disrupt services, criminals intent on stealing personal information, spies looking for intellectual property or trade secrets or nation-states searching for military and security vulnerabilities, our networks are at risk.

Cyber looting puts U.S. businesses at a competitive disadvantage, threatening jobs and our private information. The same vulnerabilities used to steal intellectual and personality property are also exploited to target America's critical infrastructure, such as our electrical grids and our banking and financial institutions. These cyber weaknesses make the intelligence-sharing provisions within H.R. 624 vitally important. However, as we seek to secure and defend the U.S. economy and our country's critical infrastructure, we must be mindful of our Nation's founding principles. We must ensure that we protect our citizens' privacy and civil liberties.

The House Permanent Select Committee on Intelligence has sought the input of and worked closely with privacy and civil liberties groups to strengthen the bill and provide necessary individual protections. These discussions resulted in a number of amendments that were adopted on a broad bipartisan basis during the committee markup.

My amendment, offered with my colleague from Connecticut (Mr. HIMES), specifically limits the private sector's use of cyber threat intelligence only to a cybersecurity purpose. This provision addresses the concerns and misperceptions that private sector companies could have used this information for marketing and other commercial purposes.

Another amendment requires the establishment of minimization procedures to limit the receipt, retention, and use of personally identifiable information, or PII. In the unlikely event that PII is inadvertently shared, this provision will prevent the government from receiving and/or maintaining that information while still ensuring rapid transmission of critical cyber threat intelligence necessary to protect our systems.

Yet another amendment narrows the authorized use of shared cyber threat intelligence by striking the provision providing the government broad authority to use this information for national security purposes.

All of these bipartisan amendments will provide the private sector the necessary tools to protect its own networks while at the same time providing critical protections for privacy and civil liberties.

This legislation represents an important first step toward securing our Nation's intellectual property and critical infrastructure from cyber attack, and I urge my colleagues to support its passage.

Again, I thank the chairman and the ranking member for their leadership.

Mr. RUPPERSBERGER. Madam Chair, I now yield 2 minutes to a senior member of our committee who worked very hard on this bill, the gentleman from California (Mr. THOMPSON). He's been with us for the last 3 years attempting to pass a bill that will help our country and protect us.

Mr. THOMPSON of California. Madam Chair, I thank the gentleman for yielding, and I thank both the ranking member and the chairman for their good work on this measure and for including all of us in trying to build a better product.

Clearly, the threat of a devastating cyber attack is real and, as has been mentioned by a number of previous speakers, can't be understated. Advanced cyber attacks from China and other nation-state actors are stealing hundreds of billions of dollars' worth of cutting-edge research and development from our U.S. companies and even from our Federal Government. That's why it's essential that the business community and the Federal Government work together to share cyber threat information for the purpose of protecting the American people from the fallout of cyber attacks and cyber hackers.

While it's important that we protect against the threat of cybersecurity, it's equally as important that we recognize the responsibility to protect the constitutional rights of law-abiding citizens. Though I support H.R. 624, both for the fact that it is important that we address these issues and because I believe it needs to be moved on and we can get it in conference committee with the Senate bill, I remain somewhat concerned that the bill as drafted could lead to the broad sharing of consumer information which in turn could be used in ways unrelated to combating cybersecurity threats.

□ 1500

I emphasize ''could be used.''

Already the chair and the ranking member have accepted and we've incorporated a series of provisions in this bill that I authored that would minimize the sharing of some personally identifiable information, that would limit permissible uses of information which would be shared under this bill, and that would insist on a number of reporting requirements that will ensure Congress' ability to provide the necessary oversight of this program.

The CHAIR. The time of the gentleman has expired.

Mr. RUPPERSBERGER. I yield the gentleman an additional 30 seconds.

Mr. THOMPSON of California. So, taken together, these provisions will improve the transparency and the accountability of this bill. However, notwithstanding these important changes, the bill is not perfect. Given the significance of this threat and the commitment of everyone to continue to work together, I strongly urge my colleagues to support this bill and to move it out of the House. Let's get the thing to conference. Let's get the best bill possible, get it signed into law, and work together to protect the American people.

Mr. ROGERS of Michigan. Madam Chair, I am proud to yield 3 minutes to a leader on the Homeland Security

Committee and the chair of the House Admin Committee, the gentlelady from Michigan (Mrs. MILLER).

Mrs. MILLER of Michigan. I thank the gentleman for yielding me time.

Madam Chair, let me just read for our colleagues the preamble of our Constitution:

We the people of the United States, in order to form a more perfect Union, establish justice, insure domestic tranquility, provide for the common defence, promote the general welfare, and secure the blessings of liberty to ourselves and our posterity, do ordain and establish this Constitution for the United States of America.

Madam Chair, this great statement that is the foundation for our Federal Government provides us the direction that we need to our primary responsibilities. I would suggest that this legislation helps us fulfill every one of the responsibilities mandated on us by our Constitution. Now let's just take them one by one.

''Establish justice''—it is just to protect American companies from the theft of their intellectual property by attackers and by competitors.

''Insure domestic tranquility''—can you even imagine the threat to domestic tranquility if our power grid is successfully attacked by a foreign state like North Korea and this Nation is left in the dark?

''Provide for the common defence''—what is more common than our power grid, our financial system and our economy? Are we not required to defend all of that?

''Promote the general welfare''—again, if our power grid is taken down, it is impossible to promote the general welfare.

''Secure the blessings of liberty to ourselves and to our posterity''—our intellectual property, made with American ingenuity, our life savings in banks, under threat from foreign actors, our jobs, our economy. All of these blessings of liberty are currently at risk if we do nothing.

I've heard some suggest, Madam Chair, that they have constitutional concerns about passing this bill. I would just suggest to them that I believe strongly that you should have constitutional concerns about not passing this bill. I do not believe that our Constitution gives foreign state actors like China or Russia or North Korea or Iran uncontested access to the critical systems of private American companies. To the contrary, I believe that our Constitution requires us, the Federal Government, to defend them.

I certainly want to applaud the great work that has been done by the chairman of the House Intelligence Committee, Mr. ROGERS of Michigan, and certainly applaud our ranking member, Mr. RUPPERSBERGER.

Gentlemen, you have worked so closely together on your committee and with other committees as well on this great piece of legislation.

I would urge all of my colleagues, Madam Chair, to join me in fulfilling our oath and in voting ''yes.''

Mr. RUPPERSBERGER. Madam Chairwoman, I yield 2 minutes to a great Member from the State of Illinois (Mr. ENYART).

Mr. ENYART. Madam Chair, I rise today in support of this important legislation.

The threat we face today from cyber attacks poses a clear and present danger that must be addressed. When I was sworn in to Congress to represent the people of southern Illinois, I took a vow to protect them from all enemies, both foreign and domestic. It was not the first time I had taken such an oath. By supporting CISPA, we move to fulfill our oath.

I know there are good Americans who oppose this legislation because they believe the protections for civil liberties and privacy don't go far enough, but we must not let the perfect be the enemy of the good. This bill prohibits the government from forcing private sector entities to provide information to the government. It places restrictions on the use of any data voluntarily shared. The bill provides for strong congressional oversight. These are tremendous victories to protect our civil liberties.

I support this bill because American jobs hang in the balance. Every day, our companies are subject to cyber attacks seeking to steal valuable trade secrets which deprive American citizens of high-paying high-tech jobs. Locally, my hometown grocery store in southern Illinois, Schnucks, was recently hacked, and customers' debit and credit card information was compromised, making many of my constituents vulnerable to theft.

I cannot stand by and let an opportunity to prevent such actions pass me by, which is why I stand in support of this legislation. To protect the jobs of those who work to build planes at Boeing in Belleville or workers at Afton Chemical in Sauget, I must support this legislation. To ensure that those who make weapons to defend our country at General Dynamics in Marion, Illinois, don't lose their jobs because some Chinese hacker has stolen proprietary information, I must support this legislation.

As the weapons of warfare change and adapt, we must make the necessary adjustments to protect our Nation while adhering to our founding principles. I urge my colleagues to join me in support of this act.

The CHAIR. The gentleman from Maryland has 14½ minutes remaining, and the gentleman from Michigan has 5½ minutes remaining.

Mr. ROGERS of Michigan. Madam Chair, I yield 2 minutes to a former military officer, the distinguished gentleman from Kansas (Mr. POMPEO).

Mr. POMPEO. I want to thank Chairman ROGERS and Ranking Member RUPPERSBERGER for all of their hard work over many months, now years, in bringing this to where we are today, and I want to thank all of the committee staff who worked so hard to bring it to this point as well.

I'd like to keep things pretty simple. If there were a sergeant from the Chinese People's Liberation Army inside one of our power plants or inside one of our banks and if they were trying to steal stuff and if they were looking around, trying to figure out how to get in and how to access our systems or to take property or to do damage to our power grid, the American people would demand that the government do whatever it could, and they would be thrilled to learn that that company was permitted and, indeed, protected if it decided to share with others that potential threat to its piece of the infrastructure. That's what we're doing today.

The world has changed just a little bit. In just this last month, the last M–1 tank left Europe. It's the first time we haven't had a tank in Europe since D-day when the great Kansan invaded on the great quest to free us from Nazi totalitarian domination. There are no tanks. We fight in a different world today. We use the word ''cyber,'' and sometimes folks forget what we're really talking about. We're talking about nation-states trying to do terrible harm to American interests, to American property and, indeed, to American civil liberties.

Now, in the last minute I have here, I want to talk about a couple of myths that have arisen about this piece of legislation. When I first learned about it, I, too, shared some of the concerns about what might be happening, about what might take place here. I offered an amendment last year, which is now incorporated into the bill, along with dozens of such amendments, to make sure belt-and-suspenders that we protected civil liberties.

I've heard the myth propagated that this piece of legislation violates contract rights, that somehow through CISPA we're going to take away the ability of people to negotiate privately for contractual things that they want. I don't know how that could be. This bill is purely voluntary. It mandates that no one participate. It simply allows businesses to voluntarily participate and share information they have about attacks that have been foisted upon them.

I've heard a second myth that this will authorize warrantless searches across the United States of America.

The CHAIR. The time of the gentleman has expired.

Mr. ROGERS of Michigan. I yield an additional 60 seconds to the gentleman.

□ 1510

Mr. POMPEO. There's talk about warrantless searches all across America. The legislation does no such thing. It's a short bill. It's 26 pages. I would urge everyone to go read it for themselves.

It fairly clearly limits what government may do, what information government may receive. It limits what private companies can share with government and amongst themselves. It

limits what government can do with that information once it is received. It has greatly capped what is going on here.

Its design is simple: it is to make sure that all of the information about direct attacks on America are widely known, easily disseminated, and available for all to help in the protection of the American state. I urge my colleagues to support this legislation.

Mr. RUPPERSBERGER. Madam Chair, I yield 2 minutes to my good friend, the gentleman from Rhode Island (Mr. LANGEVIN); and I do want to say that we've been working together for years on this issue of cybersecurity, and I consider him to be one of the experts and one of my closest friends working on this issue.

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

Mr. LANGEVIN. Madam Chair, I thank the gentleman for yielding. I rise in strong support of H.R. 624, and I do thank Chairman ROGERS and Ranking Member RUPPERSBERGER for their commitment to a bipartisan and inclusive process on a very, very challenging issue.

We know with certainty that cybersecurity threats that we face are real, and they are increasing both in number and sophistication every day. Congress may not have acted last year, but those who would use cyberspace for nefarious purposes certainly did, and they continue to steal intellectual property, identities, funds from bank accounts, and sensitive security information.

I know full well that this is not a perfect bill, such is the nature of the legislative process. But we need the authority that CISPA provides to allow the voluntary sharing of cybersecurity threat information.

Improvements, I should point out, have been made over last year's bill. Several amendments have already been adopted to alleviate many privacy concerns, and more may be adopted before we are done. I welcome such progress. This bill is an important step, but information-sharing is only one portion of the broader cybersecurity debate.

I have long maintained that we must also work to ensure the creation of minimum standards for critical infrastructure; the education of a strong and vibrant future cybersecurity workforce; and effective Federal and military cyber structure, including a Senate-confirmed cybersecurity director with real authority, including comprehensive budgetary authority; and the coordination of research and development on cybersecurity across the Nation.

Together with the President's recent executive order, I believe CISPA and the bills this House approved yesterday are a very promising beginning, but there is obviously much more to be done.

Again, I want to thank Chairman ROGERS and Ranking Member RUPPERSBERGER for their efforts. I commend them on a collaborative approach to a very important issue, and I ask my colleagues to support this important measure.

Mr. ROGERS of Michigan. I don't have any further speakers, and so I will continue to reserve the balance of my time to close.

Mr. RUPPERSBERGER. I yield 2 minutes to the gentlewoman from Illinois (Ms. SCHAKOWSKY), who is a senior member of our committee and has worked very hard on this issue.

Ms. SCHAKOWSKY. Madam Chair, I sincerely want to thank the chair and ranking member of the Intelligence Committee and express my appreciation for all of their efforts to work in a bipartisan manner and to address the concerns raised by me, by civil liberties groups, and by the White House.

However, I rise today in opposition to the bill. While I strongly believe that we need to address the serious cybersecurity threat—there is no question about that—I think we can do it without compromising our civil liberties. Despite some positive changes, I feel this bill fails to adequately safeguard the privacy of Americans. Cybersecurity and privacy are not mutually exclusive, and this bill fails to achieve a balance between protecting our networks and safeguarding our liberties.

Yesterday, I offered an amendment that would have made critical advances toward protecting privacy. My amendment would have required that companies report cyber threat information directly to civilian agencies, maintaining the longstanding tradition that the military doesn't operate on U.S. soil or collect information of American citizens.

Another important amendment offered by Congressman SCHIFF would have required companies to make ''reasonable efforts'' to remove personal information before sharing cyber threat information. Unfortunately, those critical amendments were not made in order.

Yesterday, the Obama administration expressed ongoing concerns about this legislation, issuing a veto threat. I share the President's concern—despite positive changes, this bill falls short in several key ways. As written right now, and hopefully there still may be some changes, CISPA allows the military to directly collect personal information on American citizens. It fails to safeguard privacy of Americans and grants sweeping immunity to companies for decisions made based on cyber information, prohibiting consumers from holding companies accountable for reckless actions and negligence.

The CHAIR. The time of the gentlewoman has expired.

Mr. RUPPERSBERGER. I yield 30 seconds to the gentlewoman.

Ms. SCHAKOWSKY. I do urge my colleagues to oppose this bill. We can and should do better, and I'm hopeful that we still will do better.

Mr. ROGERS of Michigan. Madam Chair, I yield myself 30 seconds.

I just want to make very, very clear—and I thank the gentlelady for working with us, she is a great member of the committee—nowhere in this bill does it allow the military to collect information on private citizens in the United States. This is not a surveillance bill. It does not allow it to happen. That needs to be very, very clear in this debate. It does not allow the military to surveil private networks in the United States. Period. End of story. That's the biggest part of our privacy protections. Again, I want to thank the gentlelady for working with us, but that's just an inaccurate statement, and I want to make that clear for the RECORD.

I reserve the balance of my time.

Mr. RUPPERSBERGER. Madam Chair, how much time do I have remaining?

The CHAIR. The gentleman from Maryland has 10 minutes remaining.

Mr. RUPPERSBERGER. Madam Chair, I yield 2 minutes to the gentlewoman from Texas (Ms. JACKSON LEE), a very active member of our caucus.

Ms. JACKSON LEE. I thank the distinguished ranking member and the chairman, as well, for working to answer an enormous concern on the question of national and domestic security.

Since Robert Tappan Morris in 1988 released one of the first commuter worms, we realized, as the computer and the Internet now have grown, the proliferation of computer malware, or computer programs designed specifically to damage computers or their networks or to co-opt systems or steal data, has attracted public and media attention and that we needed to do something. Now more than ever, cybersecurity impacts every aspect of our lives.

As a member of the Homeland Security Committee, I can assure you that my concern about the electric grid utilities, the energy and financial industries, recognize that it is important to act, and to act with speed and understanding. Likewise, I am concerned about the rage in epidemic of hackers and the impact that it has on 85 to 87 percent of the infrastructure in this Nation.

For that reason, however, I believe that along with this effort, we should have a lead civilian agency to collect the data. I'm looking forward to the manager's amendment, which I hope will clarify that Homeland Security will be that.

In addition, I have offered an amendment. My amendment ensures that if a cloud service provider identifies or detects an attempt by someone to access, to gain unauthorized access to nongovernmental information stored on the system, it would not be required or permitted to report that attempt to the government and it cannot share that information with the government. I thank the Rules Committee for allowing that amendment to be in.

I do, however, want to raise the question on privacy. I believe that we could

fix this legislation with a small addition dealing with the privacy question as we hopefully address the question dealing with the lead civilian agency. I thank the chairman and the ranking member, and I look forward to further discussion on this legislation.

Mr. ROGERS of Michigan. I continue to reserve the balance of my time.

Mr. RUPPERSBERGER. Madam Chair, I yield 2 minutes to the gentleman from Colorado (Mr. POLIS), a member of the Rules Committee.

Mr. POLIS. I thank the gentleman.

This bill, unfortunately, hurts what it purports to help. It's detrimental to job growth, innovation, and privacy.

□ 1520

We talked a bit about the process whereby a number of amendments that would have improved it were not allowed to be discussed or voted on on the floor. And there are still enormous flaws with this bill which need to be addressed.

Look, to the extent that companies believe that information-sharing is important, it should be done in a way that's consistent with sanctity of contract. If there's something that gets in the way of information-sharing, we need to identify it. That hasn't been identified.

Clearly, the answer is not to say whatever a company agrees upon with a personal user, even if explicitly it says we're going to keep your information private, the minute after that's agreed to by a user, the company would be completely indemnified by turning all this information, personal information, credit card information, address, everything, over to the government.

Now, why not remove anything?

Why not just pass along the parts that are related to cybersecurity?

There's no incentive to do so. Had there been a requirement that reasonable efforts were taken to delete personal data, that would have been a step in the right direction. But, again, it's an extra cost with no benefit for the company to delete personal data because they're completely indemnified with regard to this matter without the consent of the user himself.

What happens to this information once it reaches the government?

It can be shared with any government agency. It can be shared with the Bureau of Alcohol, Tobacco and Firearms, the National Security Agency, the Food and Drug Administration. Again, the limitations are so open-ended that anything that relates even to a minor scratch or a cut, issues completely unrelated to cybersecurity, things that could be related to dog bites, essentially any information.

Part of the problem here, there are cyber attacks everywhere. I ran an e-commerce site. Tens of thousand every day. I mean, any e-commerce company experiences this every day, so it's a reality every day. Everything is a potential cybersecurity threat. There's people cracking passwords every day.

So all information is affected by this, under this bill, in its present form, turned over to the government, shared with every agency relating to any bodily injury or harm, and we haven't been offered an opportunity to amend that.

So I encourage my colleagues to vote ''no'' on this bill. We can and we must do better for our country.

Mr. RUPPERSBERGER. I yield 2 minutes to the gentlewoman from Alabama (Ms. SEWELL). Is it ''Roll Tide''? She is an outstanding new member of the Intelligence Committee. She's smart. She works hard. She's very dynamic, and she is our closer today.

Ms. SEWELL of Alabama. Madam Chair, today I rise to support the bill.

I can say, Madam Chair, that I actually voted against the bill last term. But today I am proud to say, because of the hard work of both the chairman and the ranking member and so many members of this committee, that today I stand before you in support of the bill.

I am now a new member of the Intelligence Committee and, as I've told my staff, the more you know, the better you can vote. And today, I want to rise to explain why I am voting for this bill.

I think that everybody agrees that there are cyber threats each and every day. And, in fact, Director Clapper, the Director of National Intelligence, he actually said his number one thing that keeps him up at night is cyber attacks.

And what this bill will do is simply to share information. It is not about releasing personal identifiable information. That is strictly prohibited by this bill. So it is strictly prohibited by this bill.

And this bill has been greatly enhanced by so many of my wonderful colleagues who have submitted amendments, many of which I am sure will pass tomorrow, as well as greatly enhanced by the amendments that were brought forth by committee members.

I shared some serious concerns about some privacy protections when I came on the committee, and I have to tell you that the committee was gracious enough to listen to the amendments that I offered, as well as other amendments that were offered by my colleagues on this side of the aisle.

I was surprised, given the partisan nature of politics here in this House, that the Intelligence Committee really tries, because of our national security, to work together. And in a true bipartisan manner, many of those privacy protections were unanimously agreed to by members of the committee.

Once again, I urge my colleagues to vote for this bill, and I urge the President to sign this bill into law.

Today, I rise in support of this bill. But Madam Chair, last year, I voted against the cybersecurity bill that was offered in this body. I am now and am honored to serve as a member of the Intelligence Committee and the more you know, the better you can vote. I want to commend the Chairman and the Ranking Member for their leadership to improve this legislation. I also want to thank all of my colleagues who offered amendments to strengthen this bill by providing more privacy protections for our citizens and improving inter-agency coordination. While this is not a perfect bill, this is a step in the right direction and I am hopeful that the Senate will take up this measure and make it even stronger. It is also my hope that the White House will continue to work with us in this body's effort to be proactive instead of reactive. Madam Speaker, we simply cannot afford to wait—The threats against our national and economic security are real. Attacks against our financial, energy and communication sectors are happening every day. We have received dire warnings from our defense and intelligence officials that widespread attacks are the number one threat to our national security above all else. The Director of National Intelligence, James Clapper, has elevated cyber threats to the top of the list of national-security concerns. The National Intelligence Estimate provided evidence of widespread infiltrations of U.S. computer networks. Evidence has also emerged of spying inside the computer networks of major U.S. media, including the Wall Street Journal and New York Times. Defense and intelligence officials have grown increasingly alarmed over a relentless cyber attack campaign against U.S. banks, critical infrastructure and a host of other private entities.

We must continue to work together to find a balance between preserving privacy and protecting the security of this country from the danger of cyber attacks. Sharing cyber threat information, as provided for in this bill, is vital for combatting malicious hackers, criminals, and foreign agents. By removing the legal and regulatory barriers currently impeding the free flow of actionable information, the Cyber Intelligence Sharing and Protection Act (CISPA) will promote nimble, adaptive innovation—the best strategy for defending against a rapidly evolving threat landscape.

This growing number and complexity of cyber attacks on private and government computers has provided an opportunity for us to join together and pass bipartisan legislation to address the problem. I am committed to finding a workable solution with the Senate and White House, and I believe this bill provides a solid framework on a critical issue for national and economic security. I look forward to considering any amendments my colleagues put forth today to help improve the legislation of this bill. And though I realize this is not a perfect bill, I think the time to act is now to protect our national security. I urge members to vote for this legislation.

Mr. RUPPERSBERGER. Madam Chair, I yield myself as much time as I may consume.

First thing, we've heard testimony today about how serious the cyber attacks are to our country. We know what has occurred already. We know that our banks have been attacked, our major banks. We know that our newspapers, New York Times, Washington Post, have been attacked.

We know that news reports have said that Iran attacked Aramco, Saudi Arabia's largest oil company. They took out 30,000 computers, which means we are subjected to those attacks also.

We also know that Cyber Command has said that we, in the United States,

have lost, from the attacks on our businesses, approximately $200 billion. Just think what that equates to in jobs, stealing information about trade secrets, about competing globally with a country like China where they have all of our information, where they're able to shut down banks.

This is a very serious issue, and we need to do a better job to educate the public on how serious it is. And we just hope that we can pass this bill today in the House, a bill in the Senate, and the President signs the bill, so that we can protect our citizens, we can protect our businesses from these attacks.

If we knew that Iran was sending over an airplane with a bomb we would take it out. And yet we have to make sure that we deal with the issue in the United States of America to protect ourselves.

Now, there was a major issue raised, and that issue was privacy. And believe me, I want to say this over and over again. You don't have security if you don't have privacy. And we feel very strongly that this bill provides privacy.

But we also know, Chairman ROGERS and I know, that if we pass a bill here, we need to pass a bill in the Senate, and we need the President to sign it. So we got together, and even though we passed our bill in a bipartisan effort last year and it stalled in the Senate, we now have made the bill what we feel is a lot stronger as it deals with the perception of privacy.

And we've added oversight. We have four categories of oversight, privacy. We've made sure that minimization—taking out any privacy information that might pass—we made sure that that is 100 percent minimization so that no one's private information will pass.

But the most important thing is that we have to make sure that we pass a bill because of the fact that 80 percent of our network is controlled by 10 companies in the United States of America. And all of our experts in this area have said that if government and business can't share information about these attacks, zeros and ones, if they can't share information, they cannot protect our country from these ongoing attacks that are occurring as we speak right now.

So let's act. Let's not wait until we have another catastrophic attack like 9/11. Let's deal with this now. Let's pass the bill and make sure that we protect, again, our citizens. And I want to say it one more time. The issue that you can't have security if you don't have privacy.

I do want to also say, I want to thank all those individuals in our government, in the private sector. The privacy groups have all come together. This has been a good debate. It's been a debate about issues that the public needed to know.

And I also want to thank the chairman for his leadership, and the fact that he was willing, even though we had our bill passed a year ago, he was willing to deal with the issue of perception and to make sure we made privacy an element that we could deal with, and that we could change our bill to deal with certain perceptions. I feel that we've done that.

I also want to thank Chairman MCCAUL from Homeland Security and Ranking Member BENNIE THOMPSON from Homeland Security, who've worked with us to get an amendment that was very important, as you heard from JAN SCHAKOWSKY.

That amendment basically says that the point of entry for any communication is on the civil side of our government, Homeland Security, and we hope to pass that amendment.

And I feel very strongly that if we do that, we will have addressed the majority of the issues that are so important to this bill and to our security and to our privacy.

I yield back the balance of my time.

Mr. ROGERS of Michigan. Madam Chair, I yield myself the remaining time.

I just want to quickly, Madam Chair, address some of the moving targets on the bill. When we move to change something in the bill, the 19 privacy amendments, people who still decide they don't like it for, again, whatever reason, move their challenges of why they don't like it.

The newest, I think, straw man is that this somehow would violate contract law. Nothing in this bill allows you to avoid contract law. Nothing.

□ 1530

It's a red herring. It is not accurate. Nothing in this bill would allow this to happen. The fact that someone who was in the technical business would say this hurts job growth, that's interesting. The sheer number of companies who support this, from the Business Roundtable to the Financial Services Business Group to TechNet, who has companies like Intel Corporation, Symantec, Juniper, Oracle, EMC, social media, all stand up and say this is the right approach. It will allow us to protect our consumers of our product from foreign governments stealing their private information.

We need to understand what this bill is and what it is not. It is not a surveillance bill. Nothing in here authorizes surveillance. We're going to have an amendment to clarify that, to say it in the law so people can regain that confidence.

We argue, Read the bill. It's 27 pages. It is very clear. It is predominantly protections of your civil liberties, and it also allows companies to voluntarily share malicious source code—and that's source code that's committing a crime against their consumers and their company—with the Federal Government so they can go back overseas and find the Chinese or the Iranians or the Russians or the North Koreans who are perpetrating that crime. This bill is nothing more. It does do that.

Thanks to the ranking member and all who have gotten to this point. I look forward, Madam Chair, to the debate on the amendments, and I yield back the balance of my time.

Mr. CONYERS. Madam Chair, this week, the House of Representatives is scheduled to take up the Cyber Intelligence Sharing and Protection Act (CISPA). Among other things, the legislation would authorize open-ended sharing of threat information between certain private companies and the federal government, and grant those companies unlimited legal immunity. I—along with more than 30 civil liberties and privacy groups ranging from the ACLU to the Competitive Enterprise Institute—believe the bill is badly flawed, and will harm the privacy and civil liberties of our citizens. While the Intelligence Committee amended CISPA last week, purporting to address privacy-related issues, the changes do not ameliorate the core concerns I have with the bill.

CISPA would create a "Wild West" of information-sharing, where any "certified" private-sector entity could share information with any federal government agency for various ill-defined purposes. By allowing for the direct sharing of information between the private sector and the National Security Agency, as well as other Defense Department agencies, the legislation hastily casts aside time-tested legal prohibitions against intelligence agencies and the military from operating on U.S. soil. The bill should be amended to prevent this direct sharing with non-civilian agencies.

CISPA would also create duplicative information-sharing processes with no central oversight or accountability. Successive administrations have expended enormous resources building proper information-sharing programs at the Department of Homeland Security and the FBI; these efforts should be enhanced, not clouded by permitting the proliferation of redundant programs across the federal government.

The legislation also removes current legal protections applicable to companies that facilitate and process our private communications and share them with the government and one another. Companies sharing information would be exempt from all privacy statutes and would be relieved of liability for recklessly sharing, or deciding not to share information. Without narrowly defining the information that may be shared, limiting to whom it may be shared and why, and preserving mechanisms to provide accountability for wrongdoing, the privacy of our citizens and confidence in the trustworthiness of our electronic communications networks would be weakened. For example, the bill would not prevent a company sharing cyber threat information from including data not necessary to understanding the threat, such as private emails between family members or personal information such as medical records, in a data dump to the government.

The bill should narrowly define the categories of information that may be shared, such as malicious code or methods of defeating cybersecurity controls, and require that companies sharing the data take reasonable steps to remove information identifying individuals not involved in the threat. It is not enough to require government recipients of the data to remove the private information because it should never be sent to the government in the first place. The bill therefore should be amended to require that companies sharing cyber threat information make reasonable efforts to

remove such personally identifiable information from the data they share with other companies and the government.

The bill's liability protection provisions are also unnecessarily broad and eliminate the ability of aggrieved citizens and companies to protect and secure their privacy, as well as their property and physical well-being. Regardless of whether a company acted recklessly or negligently, the bill would prevent civil or criminal actions for decisions made for cybersecurity purposes "based on" cyber threat information. In effect, the legislation removes critical incentives for industry to act reasonably concerning cyber threat information.

Consider a situation in which a telecommunications company through its operations becomes aware of a cyber threat directed toward a utility but fails to notify the critical infrastructure company of the threat, denying the utility the opportunity to engage in defensive measures and resulting in a catastrophic event producing substantial property damage and loss of life. Under the legislation, the telecommunications company characterizing its decision not to notify as one made for a cybersecurity purpose would be able to avoid legal liability. The bill's exemption from liability should therefore be narrowed to exclude protection for such decisions.

The cyber threats our nation faces are serious, and we need to take action. The president's recent executive order directing the enhanced sharing of cyber threat information by the government to industry is a significant step in the right direction. Legislation encouraging information-sharing by the private sector is also required, but it must be carefully crafted and limited to actual threats. The House version of CISPA is not the right solution to this real problem, and it must be fixed before it reaches the president's desk.

The CHAIR. All time for general debate has expired.

Pursuant to the rule, the bill shall be considered for amendment under the 5-minute rule.

In lieu of the amendment in the nature of a substitute recommended by the Permanent Select Committee on Intelligence, printed in the bill, it shall be in order to consider as an original bill for the purpose of amendment under the 5-minute rule an amendment in the nature of a substitute consisting of the text of Rules Committee Print 113–7. That amendment in the nature of a substitute shall be considered as read.

The text of the amendment in the nature of a substitute is as follows:

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

H.R. 624

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Cyber Intelligence Sharing and Protection Act''.

SEC. 2. CYBER THREAT INTELLIGENCE AND INFORMATION SHARING.

(a) IN GENERAL.—Title XI of the National Security Act of 1947 (50 U.S.C. 442 et seq.) is amended by adding at the end the following new section:

''CYBER THREAT INTELLIGENCE AND INFORMATION SHARING

''SEC. 1104. (a) INTELLIGENCE COMMUNITY SHARING OF CYBER THREAT INTELLIGENCE WITH PRIVATE SECTOR AND UTILITIES.—

''(1) IN GENERAL.—The Director of National Intelligence shall establish procedures to allow elements of the intelligence community to share cyber threat intelligence with private-sector entities and utilities and to encourage the sharing of such intelligence.

''(2) SHARING AND USE OF CLASSIFIED INTELLIGENCE.—The procedures established under paragraph (1) shall provide that classified cyber threat intelligence may only be—

''(A) shared by an element of the intelligence community with—

''(i) a certified entity; or

''(ii) a person with an appropriate security clearance to receive such cyber threat intelligence;

''(B) shared consistent with the need to protect the national security of the United States; and

''(C) used by a certified entity in a manner which protects such cyber threat intelligence from unauthorized disclosure.

''(3) SECURITY CLEARANCE APPROVALS.—The Director of National Intelligence shall issue guidelines providing that the head of an element of the intelligence community may, as the head of such element considers necessary to carry out this subsection—

''(A) grant a security clearance on a temporary or permanent basis to an employee or officer of a certified entity;

''(B) grant a security clearance on a temporary or permanent basis to a certified entity and approval to use appropriate facilities; and

''(C) expedite the security clearance process for a person or entity as the head of such element considers necessary, consistent with the need to protect the national security of the United States.

''(4) NO RIGHT OR BENEFIT.—The provision of information to a private-sector entity or a utility under this subsection shall not create a right or benefit to similar information by such entity or such utility or any other private-sector entity or utility.

''(5) RESTRICTION ON DISCLOSURE OF CYBER THREAT INTELLIGENCE.—Notwithstanding any other provision of law, a certified entity receiving cyber threat intelligence pursuant to this subsection shall not further disclose such cyber threat intelligence to another entity, other than to a certified entity or other appropriate agency or department of the Federal Government authorized to receive such cyber threat intelligence.

''(b) USE OF CYBERSECURITY SYSTEMS AND SHARING OF CYBER THREAT INFORMATION.—

''(1) IN GENERAL.—

''(A) CYBERSECURITY PROVIDERS.—Notwithstanding any other provision of law, a cybersecurity provider, with the express consent of a protected entity for which such cybersecurity provider is providing goods or services for cybersecurity purposes, may, for cybersecurity purposes—

''(i) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such protected entity; and

''(ii) share such cyber threat information with any other entity designated by such protected entity, including, if specifically designated, the Federal Government.

''(B) SELF-PROTECTED ENTITIES.—Notwithstanding any other provision of law, a self-protected entity may, for cybersecurity purposes—

''(i) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such self-protected entity; and

''(ii) share such cyber threat information with any other entity, including the Federal Government.

''(2) SHARING WITH THE FEDERAL GOVERNMENT.—

''(A) INFORMATION SHARED WITH THE NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER OF THE DEPARTMENT OF HOMELAND SECURITY.—Subject to the use and protection of information requirements under paragraph (3), the head of a department or agency of the Federal Government receiving cyber threat information in accordance with paragraph (1) shall provide such cyber threat information in as close to real time as possible to the National Cybersecurity and Communications Integration Center of the Department of Homeland Security.

''(B) REQUEST TO SHARE WITH ANOTHER DEPARTMENT OR AGENCY OF THE FEDERAL GOVERNMENT.—An entity sharing cyber threat information that is provided to the National Cybersecurity and Communications Integration Center of the Department of Homeland Security under subparagraph (A) or paragraph (1) may request the head of such Center to, and the head of such Center may, provide such information in as close to real time as possible to another department or agency of the Federal Government.

''(3) USE AND PROTECTION OF INFORMATION.—Cyber threat information shared in accordance with paragraph (1)—

''(A) shall only be shared in accordance with any restrictions placed on the sharing of such information by the protected entity or self-protected entity authorizing such sharing, including appropriate anonymization or minimization of such information and excluding limiting a department or agency of the Federal Government from sharing such information with another department or agency of the Federal Government in accordance with this section;

''(B) may not be used by an entity to gain an unfair competitive advantage to the detriment of the protected entity or the self-protected entity authorizing the sharing of information;

''(C) may only be used by a non-Federal recipient of such information for a cybersecurity purpose;

''(D) if shared with the Federal Government—

''(i) shall be exempt from disclosure under section 552 of title 5, United States Code (commonly known as the 'Freedom of Information Act');

''(ii) shall be considered proprietary information and shall not be disclosed to an entity outside of the Federal Government except as authorized by the entity sharing such information;

''(iii) shall not be used by the Federal Government for regulatory purposes;

''(iv) shall not be provided by the department or agency of the Federal Government receiving such cyber threat information to another department or agency of the Federal Government under paragraph (2)(A) if—

''(I) the entity providing such information determines that the provision of such information will undermine the purpose for which such information is shared; or

''(II) unless otherwise directed by the President, the head of the department or agency of the Federal Government receiving such cyber threat information determines that the provision of such information will undermine the purpose for which such information is shared; and

''(v) shall be handled by the Federal Government consistent with the need to protect sources and methods and the national security of the United States; and

''(E) shall be exempt from disclosure under a State, local, or tribal law or regulation that requires public disclosure of information by a public or quasi-public entity.

''(4) EXEMPTION FROM LIABILITY.—

''(A) EXEMPTION.—No civil or criminal cause of action shall lie or be maintained in Federal or State court against a protected entity, self-protected entity, cybersecurity provider, or an officer, employee, or agent of a protected entity, self-protected entity, or cybersecurity provider, acting in good faith—

''(i) for using cybersecurity systems to identify or obtain cyber threat information or for sharing such information in accordance with this section; or

''(ii) for decisions made for cybersecurity purposes and based on cyber threat information

identified, obtained, or shared under this section.

''(B) LACK OF GOOD FAITH.—For purposes of the exemption from liability under subparagraph (A), a lack of good faith includes any act or omission taken with intent to injure, defraud, or otherwise endanger any individual, government entity, private entity, or utility.

''(5) RELATIONSHIP TO OTHER LAWS REQUIRING THE DISCLOSURE OF INFORMATION.—The submission of information under this subsection to the Federal Government shall not satisfy or affect—

''(A) any requirement under any other provision of law for a person or entity to provide information to the Federal Government; or

''(B) the applicability of other provisions of law, including section 552 of title 5, United States Code (commonly known as the 'Freedom of Information Act'), with respect to information required to be provided to the Federal Government under such other provision of law.

''(6) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to provide new authority to—

''(A) a cybersecurity provider to use a cybersecurity system to identify or obtain cyber threat information from a system or network other than a system or network owned or operated by a protected entity for which such cybersecurity provider is providing goods or services for cybersecurity purposes; or

''(B) a self-protected entity to use a cybersecurity system to identify or obtain cyber threat information from a system or network other than a system or network owned or operated by such self-protected entity.

''(c) FEDERAL GOVERNMENT USE OF INFORMATION.—

''(1) LIMITATION.—The Federal Government may use cyber threat information shared with the Federal Government in accordance with subsection (b)—

''(A) for cybersecurity purposes;

''(B) for the investigation and prosecution of cybersecurity crimes;

''(C) for the protection of individuals from the danger of death or serious bodily harm and the investigation and prosecution of crimes involving such danger of death or serious bodily harm; or

''(D) for the protection of minors from child pornography, any risk of sexual exploitation, and serious threats to the physical safety of minors, including kidnapping and trafficking and the investigation and prosecution of crimes involving child pornography, any risk of sexual exploitation, and serious threats to the physical safety of minors, including kidnapping and trafficking, and any crime referred to in section 2258A(a)(2) of title 18, United States Code.

''(2) AFFIRMATIVE SEARCH RESTRICTION.—The Federal Government may not affirmatively search cyber threat information shared with the Federal Government under subsection (b) for a purpose other than a purpose referred to in paragraph (1).

''(3) ANTI-TASKING RESTRICTION.—Nothing in this section shall be construed to permit the Federal Government to—

''(A) require a private-sector entity or utility to share information with the Federal Government; or

''(B) condition the sharing of cyber threat intelligence with a private-sector entity or utility on the provision of cyber threat information to the Federal Government.

''(4) PROTECTION OF SENSITIVE PERSONAL DOCUMENTS.—The Federal Government may not use the following information, containing information that identifies a person, shared with the Federal Government in accordance with subsection (b) unless such information is used in accordance with the policies and procedures established under paragraph (7):

''(A) Library circulation records.

''(B) Library patron lists.

''(C) Book sales records.

''(D) Book customer lists.

''(E) Firearms sales records.

''(F) Tax return records.

''(G) Educational records.

''(H) Medical records.

''(5) NOTIFICATION OF NON-CYBER THREAT INFORMATION.—If a department or agency of the Federal Government receiving information pursuant to subsection (b)(1) determines that such information is not cyber threat information, such department or agency shall notify the entity or provider sharing such information pursuant to subsection (b)(1).

''(6) RETENTION AND USE OF CYBER THREAT INFORMATION.—No department or agency of the Federal Government shall retain or use information shared pursuant to subsection (b)(1) for any use other than a use permitted under subsection (c)(1).

''(7) PRIVACY AND CIVIL LIBERTIES.—

''(A) POLICIES AND PROCEDURES.—The Director of National Intelligence, in consultation with the Secretary of Homeland Security and the Attorney General, shall establish and periodically review policies and procedures governing the receipt, retention, use, and disclosure of non-publicly available cyber threat information shared with the Federal Government in accordance with subsection (b)(1). 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 Director of National Intelligence shall, consistent with the need to protect sources and methods, 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 subsection (b)(1) shall—

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

''(ii) promptly notify the Director of National Intelligence, the Attorney General, and the congressional intelligence committees of any significant violations of such policies and procedures.

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

''(d) FEDERAL GOVERNMENT LIABILITY FOR VIOLATIONS OF RESTRICTIONS ON THE DISCLOSURE, USE, AND PROTECTION OF VOLUNTARILY SHARED INFORMATION.—

''(1) IN GENERAL.—If a department or agency of the Federal Government intentionally or willfully violates subsection (b)(3)(D) or subsection (c) with respect to the disclosure, use, or protection of voluntarily shared cyber threat information shared under this section, the United States shall be liable to a person adversely affected by such violation in an amount equal to the sum of—

''(A) the actual damages sustained by the person as a result of the violation or $1,000, whichever is greater; and

''(B) the costs of the action together with reasonable attorney fees as determined by the court.

''(2) VENUE.—An action to enforce liability created under this subsection may be brought in the district court of the United States in—

''(A) the district in which the complainant resides;

''(B) the district in which the principal place of business of the complainant is located;

''(C) the district in which the department or agency of the Federal Government that disclosed the information is located; or

''(D) the District of Columbia.

''(3) STATUTE OF LIMITATIONS.—No action shall lie under this subsection unless such action is commenced not later than two years after the date of the violation of subsection (b)(3)(D) or subsection (c) that is the basis for the action.

''(4) EXCLUSIVE CAUSE OF ACTION.—A cause of action under this subsection shall be the exclusive means available to a complainant seeking a remedy for a violation of subsection (b)(3)(D) or subsection (c).

''(e) REPORTS ON INFORMATION SHARING.—

''(1) INSPECTOR GENERAL REPORT.—The Inspector General of the Intelligence Community, in consultation with the Inspector General of the Department of Justice, the Inspector General of the Department of Defense, and the Privacy and Civil Liberties Oversight Board, shall annually submit to the congressional intelligence committees a report containing a review of the use of information shared with the Federal Government under this section, 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 this section;

''(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 for improvements or modifications to the authorities under this section.

''(2) PRIVACY AND CIVIL LIBERTIES OFFICERS REPORT.—The Civil Liberties Protection Officer of the Office of the Director of National Intelligence and the Chief Privacy and Civil Liberties Officer of the Department of Justice, 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 this section, 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 this section. 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 this section.

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

''(f) FEDERAL PREEMPTION.—This section supersedes any statute of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under subsection (b).

''(g) SAVINGS CLAUSES.—

''(1) EXISTING AUTHORITIES.—Nothing in this section shall be construed to limit any other authority to use a cybersecurity system or to identify, obtain, or share cyber threat intelligence or cyber threat information.

''(2) LIMITATION ON MILITARY AND INTELLIGENCE COMMUNITY INVOLVEMENT IN PRIVATE AND PUBLIC SECTOR CYBERSECURITY EFFORTS.—Nothing in this section shall be construed to provide additional authority to, or modify an existing authority of, the Department of Defense or the National Security Agency or any other element of the intelligence community to control, modify, require, or otherwise direct the cybersecurity efforts of a private-sector entity or a component of the Federal Government or a State, local, or tribal government.

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

''(A) limit or modify an existing information sharing relationship;

''(B) prohibit a new information sharing relationship;

''(C) require a new information sharing relationship between the Federal Government and a private-sector entity or utility;

''(D) modify the authority of a department or agency of the Federal Government to protect sources and methods and the national security of the United States; or

''(E) preclude the Federal Government from requiring an entity to report significant cyber incidents if authorized or required to do so under another provision of law.

''(4) LIMITATION ON FEDERAL GOVERNMENT USE OF CYBERSECURITY SYSTEMS.—Nothing in this section shall be construed to provide additional authority to, or modify an existing authority of, any entity to use a cybersecurity system owned or controlled by the Federal Government on a private-sector system or network to protect such private-sector system or network.

''(5) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this section shall be construed to subject a protected entity, self-protected entity, cyber security provider, or an officer, employee, or agent of a protected entity, self-protected entity, or cybersecurity provider, to liability for choosing not to engage in the voluntary activities authorized under this section.

''(6) USE AND RETENTION OF INFORMATION.—Nothing in this section shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use information shared pursuant to subsection (b)(1) for any use other than a use permitted under subsection (c)(1).

''(h) DEFINITIONS.—In this section:

''(1) AVAILABILITY.—The term 'availability' means ensuring timely and reliable access to and use of information.

''(2) CERTIFIED ENTITY.—The term 'certified entity' means a protected entity, self-protected entity, or cybersecurity provider that—

''(A) possesses or is eligible to obtain a security clearance, as determined by the Director of National Intelligence; and

''(B) is able to demonstrate to the Director of National Intelligence that such provider or such entity can appropriately protect classified cyber threat intelligence.

''(3) CONFIDENTIALITY.—The term 'confidentiality' means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

''(4) CYBER THREAT INFORMATION.—

''(A) IN GENERAL.—The term 'cyber threat information' means information directly pertaining to—

''(i) a vulnerability of a system or network of a government or private entity or utility;

''(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or utility or any information stored on, processed on, or transiting such a system or network;

''(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network of a government or private entity or utility; or

''(iv) efforts to gain unauthorized access to a system or network of a government or private entity or utility, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network of a government or private entity or utility.

''(B) EXCLUSION.—Such term does not include information pertaining to efforts to gain unauthorized access to a system or network of a government or private entity or utility that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

''(5) CYBER THREAT INTELLIGENCE.—

''(A) IN GENERAL.—The term 'cyber threat intelligence' means intelligence in the possession of an element of the intelligence community directly pertaining to—

''(i) a vulnerability of a system or network of a government or private entity or utility;

''(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or utility or any information stored on, processed on, or transiting such a system or network;

''(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network of a government or private entity or utility; or

''(iv) efforts to gain unauthorized access to a system or network of a government or private entity or utility, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network of a government or private entity or utility.

''(B) EXCLUSION.—Such term does not include intelligence pertaining to efforts to gain unauthorized access to a system or network of a government or private entity or utility that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

''(6) CYBERSECURITY CRIME.—The term 'cybersecurity crime' means—

''(A) a crime under a Federal or State law that involves—

''(i) efforts to deny access to or degrade, disrupt, or destroy a system or network;

''(ii) efforts to gain unauthorized access to a system or network; or

''(iii) efforts to exfiltrate information from a system or network without authorization; or

''(B) the violation of a provision of Federal law relating to computer crimes, including a violation of any provision of title 18, United States Code, created or amended by the Computer Fraud and Abuse Act of 1986 (Public Law 99–474).

''(7) CYBERSECURITY PROVIDER.—The term 'cybersecurity provider' means a non-Federal entity that provides goods or services intended to be used for cybersecurity purposes.

''(8) CYBERSECURITY PURPOSE.—

''(A) IN GENERAL.—The term 'cybersecurity purpose' means the purpose of ensuring the integrity, confidentiality, or availability of, or safeguarding, a system or network, including protecting a system or network from—

''(i) a vulnerability of a system or network;

''(ii) a threat to the integrity, confidentiality, or availability of a system or network or any information stored on, processed on, or transiting such a system or network;

''(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network; or

''(iv) efforts to gain unauthorized access to a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network.

''(B) EXCLUSION.—Such term does not include the purpose of protecting a system or network from efforts to gain unauthorized access to such system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

''(9) CYBERSECURITY SYSTEM.—

''(A) IN GENERAL.—The term 'cybersecurity system' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or safeguard, a system or network, including protecting a system or network from—

''(i) a vulnerability of a system or network;

''(ii) a threat to the integrity, confidentiality, or availability of a system or network or any information stored on, processed on, or transiting such a system or network;

''(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network; or

''(iv) efforts to gain unauthorized access to a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network.

''(B) EXCLUSION.—Such term does not include a system designed or employed to protect a system or network from efforts to gain unauthorized access to such system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

''(10) INTEGRITY.—The term 'integrity' means guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.

''(11) PROTECTED ENTITY.—The term 'protected entity' means an entity, other than an individual, that contracts with a cybersecurity provider for goods or services to be used for cybersecurity purposes.

''(12) SELF-PROTECTED ENTITY.—The term 'self-protected entity' means an entity, other than an individual, that provides goods or services for cybersecurity purposes to itself.

''(13) UTILITY.—The term 'utility' means an entity providing essential services (other than law enforcement or regulatory services), including electricity, natural gas, propane, telecommunications, transportation, water, or wastewater services.''.

(b) PROCEDURES AND GUIDELINES.—The Director of National Intelligence shall—

(1) not later than 60 days after the date of the enactment of this Act, establish procedures under paragraph (1) of section 1104(a) of the National Security Act of 1947, as added by subsection (a) of this section, and issue guidelines under paragraph (3) of such section 1104(a);

(2) in establishing such procedures and issuing such guidelines, consult with the Secretary of Homeland Security to ensure that such procedures and such guidelines permit the owners and operators of critical infrastructure to receive all appropriate cyber threat intelligence (as defined in section 1104(h)(5) of such Act, as added by subsection (a)) in the possession of the Federal Government; and

(3) following the establishment of such procedures and the issuance of such guidelines, expeditiously distribute such procedures and such guidelines to appropriate departments and agencies of the Federal Government, private-sector entities, and utilities (as defined in section 1104(h)(13) of such Act, as added by subsection (a)).

(c) PRIVACY AND CIVIL LIBERTIES POLICIES AND PROCEDURES.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the Secretary of Homeland Security and the Attorney General, shall establish the policies and procedures required under section 1104(c)(7)(A) of the National Security Act of 1947, as added by subsection (a) of this section.

(d) INITIAL REPORTS.—The first reports required to be submitted under paragraphs (1) and (2) of subsection (e) of section 1104 of the National Security Act of 1947, as added by subsection (a) of this section, shall be submitted not later than 1 year after the date of the enactment of this Act.

(e) TABLE OF CONTENTS AMENDMENT.—The table of contents in the first section of the National Security Act of 1947 is amended by adding at the end the following new item:

''Sec. 1104. Cyber threat intelligence and information sharing.''.

SEC. 3. SUNSET.

Effective on the date that is 5 years after the date of the enactment of this Act—

(1) section 1104 of the National Security Act of 1947, as added by section 2(a) of this Act, is repealed; and

(2) the table of contents in the first section of the National Security Act of 1947, as amended by section 2(d) of this Act, is amended by striking the item relating to section 1104, as added by such section 2(d).

The CHAIR. No amendment to that amendment in the nature of a substitute shall be in order except those printed in House Report 113–41. Each such amendment may be offered only in the order printed in the report, by a Member designated in the report, shall be considered as read, shall be debatable for the time specified in the report equally divided and controlled by the proponent and an opponent, shall not be subject to amendment, and shall not be subject to a demand for division of the question.

AMENDMENT NO. 1 OFFERED BY MR. ROGERS OF MICHIGAN

The CHAIR. It is now in order to consider amendment No. 1 printed in House Report 113–41.

Mr. ROGERS of Michigan. Madam Chair, I have an amendment at the desk.

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 12, beginning line 15, strike ''unless such information is used in accordance with the policies and procedures established under paragraph (7)''.

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

The Chair recognizes the gentleman from Michigan.

Mr. ROGERS of Michigan. I offer this amendment to ensure that library records, firearm sales records, medical records, and tax returns are not included in any information voluntarily shared with the government under CISPA. Though the underlying bill would not permit this information unless it was cyber threat information, I will support this amendment, as it is a clarification amendment that settles some Members' concerns and reflects an amendment that was passed last year overwhelmingly.

With that, Madam Chair, I urge this body's support of this clarification amendment, and I reserve the balance of my time.

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

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

There was no objection.

Mr. RUPPERSBERGER. I support Chairman ROGERS' amendment to make a technical change to correct our personal records provision and retain the privacy protections that we had in our bill upon the introduction.

I yield back the balance of my time.

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

The CHAIR. The question is on the amendment offered by the gentleman from Michigan (Mr. ROGERS).

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

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

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

AMENDMENT NO. 2 OFFERED BY MR. CONNOLLY

The CHAIR. It is now in order to consider amendment No. 2 printed in House Report 113–41.

Mr. CONNOLLY. Madam Chairwoman, I have an amendment at the desk.

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 2, line 15, strike ''and''.

Page 2, line 18, strike the period and insert ''; and''.

Page 2, after line 18, insert the following:

''(D) used, retained, or further disclosed by a certified entity for cybersecurity purposes.''.

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

The Chair recognizes the gentleman from Virginia.

Mr. CONNOLLY. Madam Chairwoman, this amendment represents a commonsense improvement to H.R. 624, which I support, that simply narrows the scope of the authorization for the intelligence community to share classified—I stress, classified—cyber threat intelligence with private sector entities and utilities.

As my colleagues are aware, the administration and some leading voices from the civil liberties and privacy rights communities have raised serious concerns with CISPA as reported out of the Permanent Select Committee on Intelligence. These concerns revolve around the fact that many provisions of CISPA are perhaps perceived as overly vague, or outright silent, with respect to limiting the scope of information sharing and mitigating the risk of unintended consequences.

For example, section 2 of CISPA, titled ''Cyber Threat Intelligence and Information Sharing,'' is silent on what specific purposes classified cyber threat intelligence may be used, retained, or further disclosed by a certified entity. As reported, section 2 only requires that the DNI's procedures governing the sharing of classified cyber threat intelligence between the intelligence community and private sector entities be ''consistent with the need to protect the national security of the United States'' and used by certified entities ''in a manner which protects cyber threat intelligence from unauthorized disclosure.''

In this particular instance, I believe the concerns raised over the potential unintentional consequences from vagueness are real, valid, and ought to be addressed. I also believe it's a false choice that we must somehow choose between effective cybersecurity initiatives on the one hand and preserving the sacred civil liberties and privacy rights we hold so dear as a Nation on the other. In many cases, defining or limiting the scope of authority would go a long way toward addressing the privacy concerns that have been raised with respect to this legislation.

To be clear, I want to recognize that the sponsors of CISPA have already engaged in good faith efforts to incorporate and address outstanding concerns with respect to the legislation that were held by the administration and other stakeholders, and I think that needs to be recognized.

On that note, I am pleased that my amendment that was made in order represents a straightforward improvement, I hope, to CISPA that's consistent with the sponsor's stated commitment to enhancing cybersecurity, safeguarding privacy rights and civil liberties, and ensuring oversight of activity. The amendment simply establishes that, with respect to CISPA's requirements, the DNI establish procedures to govern the sharing of classified cyber threat intelligence—that this classified cyber threat intelligence may only be used, retained, or further disclosed by a certified entity for cybersecurity purposes.

As noted by the ACLU in its statement of support for the amendment, it's consistent with similar restrictions limiting the scope of other information sharing activities addressed in other parts of the bill. The straightforward enhancement will be one of many needed improvements to the bill that will ensure it is a targeted, well-defined bill that directly—and only—strengthens our national cybersecurity.

With that, I reserve the balance of my time.

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

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

Mr. ROGERS of Michigan. Madam Chair, I do not oppose this amendment, which clarifies that classified intelligence shared by the government with a certified cybersecurity entity may only be used, retained, or further disclosed for cybersecurity purposes. The amendment is consistent with language that is already in the bill requiring the DNI, the Director of National Intelligence, to ensure that such classified information is carefully protected.

I appreciate the gentleman's working with us and the ACLU to find an amendment that we could all agree on. I do not oppose this further clarification and would urge support by this body of the amendment.

I reserve the balance of my time.

Mr. CONNOLLY. I would inquire of the Chair how much time is remaining.

The CHAIR. The gentleman from Virginia has 2 minutes remaining.

Mr. CONNOLLY. Madam Chairwoman, I yield 1 minute to the distinguished ranking member of the committee, the gentleman from Maryland (Mr. RUPPERSBERGER).

□ 1540

Mr. RUPPERSBERGER. I thank the gentleman for yielding.

This amendment increases the privacy and civil liberties protections in our bill; therefore, I urge a ''yes'' on Congressman CONNOLLY's amendment.

Mr. ROGERS of Michigan. I continue to reserve the balance of my time.

Mr. CONNOLLY. Madam Chairwoman, I yield 1 minute to my distinguished colleague and our friend from Georgia (Mr. JOHNSON).

Mr. JOHNSON of Georgia. Madam Chair, I rise in support of this amendment.

I would also argue that, in addition to it being vague, it's also overbroad in that it includes investigations for child pornography and child abductions and computer crimes. This means that under CISPA, the NSA could share data with law enforcement to investigate computer crimes, which is so broad and includes even lying about your age on your Facebook page. Are these really cyber threats that this bill claims to fix? We must defend against cyber attacks while protecting the liberties and privacy of Americans.

Mr. ROGERS of Michigan. Madam Chair, I yield myself such time as I may consume to clarify that this doesn't call for investigations of those crimes based on this material, but only protection of the individuals that may—and I want to stress ''may,'' because, again, the PII, the personal identifying information, is stripped clean. But in some rare, rare cases, you might find that you have located the child who has been subjugated to child pornography. In those cases, you don't want to throw that away. There are parents out there begging for us to find this child. It's very rare, it's exceptional, doesn't happen often, but in that very rare case—and, remember, there's no personally identifiable information. It would allow for the protection, not investigation.

I reserve the balance of my time.

Mr. CONNOLLY. Madam Chairwoman, I just want to thank the distinguished chairman and the distinguished ranking member of the committee for their leadership and for their cooperation, and I yield back the balance of my time.

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

The CHAIR. The question is on the amendment offered by the gentleman from Virginia (Mr. CONNOLLY).

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

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

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

AMENDMENT NO. 3 OFFERED BY MR. SCHNEIDER

The CHAIR. It is now in order to consider amendment No. 3 printed in House Report 113–41.

Mr. SCHNEIDER. Madam Chairman, I have an amendment at the desk.

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 3, beginning on line 2, strike ''employee or officer'' and insert ''employee, independent contractor, or officer''.

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

The Chair recognizes the gentleman from Illinois.

Mr. SCHNEIDER. Every day, U.S. Web sites, databases, and operating networks are threatened by foreign governments, criminal organizations, and other groups trying to hack into our systems and wreak havoc.

Daily we read about infiltrations of the networks of our banks, newspapers, and even Federal agencies putting sensitive information at risk. These cyber attacks are real, and they can have devastating consequences: billions of dollars a year in stolen intellectual property and the potential to shut down our power grids and financial systems. The Cyber Intelligence Sharing and Protection Act gives the private sector the necessary tools to protect itself and its customers against these cyber attacks.

Currently, the intelligence community has the ability to detect cyber threats, but Federal law prohibits the sharing of this information with the very companies whose firewalls are under attack. By sharing this information, private companies can actually prevent these attacks.

The amendment I'm offering makes a small, clarifying change to the underlying bill, simply allowing independent contractors to be eligible for security clearances to perform the critical work of handling cyber threat intelligence. This clarification will allow companies—in particular, small and medium-sized businesses without the resources to employ full-time experts—to hire the most capable individuals and organizations to analyze network information, coordinate with the Federal Government, and protect ordinary Americans.

We cannot allow ourselves to be in a situation where the Federal Government has available the information to prevent or mitigate a cyber attack, but companies remain defenseless because there was no legal framework to share that critical information.

The networks at risk power our homes, our small businesses, and are what allow our banking systems to function. They facilitate nearly every aspect of our daily lives. These networks must be protected as best and responsibly as possible.

I urge my colleagues to support both my amendment and final passage of this critically important bill.

I reserve the balance of my time.

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

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

There was no objection.

Mr. ROGERS of Michigan. Madam Chairman, I will support the clarification in this amendment.

The amendment clarifies that independent contractors are eligible to receive security clearances to handle cyber threat intelligence and cyber threat information shared under the bill, an important clarification amendment.

I appreciate the gentleman's work and effort in offering this amendment; And because the bill was not intended to exclude independent contractors, I will support this important clarification and would reserve the balance of my time.

Mr. SCHNEIDER. I yield such time as he may consume to the gentleman from California (Mr. SCHIFF).

Mr. SCHIFF. I thank the gentleman for yielding, and I rise in opposition to the overall measure.

There are three concerns that have been raised by the administration about this bill that I share.

The first is that it does not include a provision requiring the private sector to make reasonable efforts to remove personal information before they share it with each other or before they share it with the government. This is a bedrock necessity for those who are concerned about the privacy of Americans who may be implicated in this cyber sharing.

Second, it's very important that a civilian agency, like the Department of Homeland Security, be the main intake—really, the sole intake—for this domestic data.

There was one form of amendment offered in Rules to try to address this problem yesterday, yet another form of that amendment that was ultimately adopted by Rules, and yet a third form of that amendment that was adopted here this morning. None of us know exactly what it does because it has been a moving object. But it is very unclear whether this amendment would make a civilian agency, such as DHS, the sole intake for this domestic data. It should not be a military agency. We shouldn't have the private sector interacting directly with a military agency when it comes to domestic data that may involve the privacy of the American people.

Finally, the immunity provisions are very broad and need to be reined in so as to encourage the private sector to take reasonable steps to make sure it

does not compromise privacy interests when it is not necessary to do so to protect cybersecurity.

Those three issues still must be addressed.

I want to compliment the chairman and the ranking member for the work they have done. They have made a very good-faith effort to make progress on many of these issues and in fact have made progress, but the bill still falls short and I must urge a ''no'' vote.

Mr. SCHNEIDER. Madam Chairman, may I inquire as to how much time I have remaining.

The CHAIR. The gentleman from Illinois has 2 minutes remaining.

Mr. SCHNEIDER. I yield such time as he may consume to the ranking member.

Mr. RUPPERSBERGER. Madam Chair, our bill now enables companies and the government to have the option to hire independent contractors to handle cyber threat information. It helps bring talented people into our cybersecurity workforce; it provides jobs; it is good for our economy; and it is good for our national security. Therefore, I urge a ''yes'' vote on this amendment.

I also want to acknowledge Congressman SCHNEIDER for his involvement in this issue.

Mr. SCHNEIDER. I reserve the balance of my time.

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

I just want to address my friend from California, who is a thoughtful member of the intelligence community.

This is a position that much has been debated about: Should the government regulate into the private sector their use of the Internet? I argue that is a dangerous place to go. They will have to promulgate rules; they will have to set what reasonable standards are; they will have to determine what the private sector does on the Internet. That's government in the Internet. One of the things that we decided to avoid in this bill was not to make that mandate, the burden to make sure that no PII, personal identifying information, is mandated in this bill; and it's stripped out at the place where the burden should be: on the government. To make sure it happens, we have four different layers of oversight built in just to make sure what we say that they're supposed to do according to the law, they follow the law—four levels of review.

□ 1550

We shouldn't put the burden on the victims. We don't do it if somebody sticks a gun in your face on the street or robs the bank or robs your home. What's the difference if they're robbing your Internet or stealing your blueprints that steals American jobs? The difference? There is none. Theft is theft.

Let us not move to get the government into regulating. Aspects of the Internet between private to private has been the explosion of growth in one-sixth of our economy. Keep the government out of it.

That's what we decided to do. We came to a very sensible place that protects that PII, that personal identifying information, and allows the government to stay out of regulating the Internet.

I think that's the right prudent course. I think most Americans are with us. Certainly the broad specter of industries who have joined this, from the high-tech industry to the financial services to manufacturing, have said, This is the right way to go. You stay out of our business. We'll share with you when we're victims of a crime.

With that, I reserve the balance of my time.

Mr. SCHNEIDER. Madam Chairman, I just want to thank the ranking member and the chairman for the way you have approached this in a bipartisan effort, and I yield back the balance of my time.

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

The CHAIR. The question is on the amendment offered by the gentleman from Illinois (Mr. SCHNEIDER).

The amendment was agreed to.

AMENDMENT NO. 4 OFFERED BY MR. LANGEVIN

The CHAIR. It is now in order to consider amendment No. 4 printed in House Report 113–41.

Mr. LANGEVIN. Madam Chair, I rise to offer an amendment, No. 35, listed as No. 4 in the rule.

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 8, line 16, strike ''a State, local, or tribal law or regulation'' and insert ''a law or regulation of a State, political subdivision of a State, or a tribe''.

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

The Chair recognizes the gentleman from Rhode Island.

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

My amendment ensures that utility districts are not unnecessarily and unintentionally limited from protecting their own information and ultimately will lead to a broader and more effective information sharing structure, leading to better cybersecurity across all critical infrastructure. Specifically, the amendment replaces the word ''local,'' which is typically interpreted to mean city, town, and county by the courts.

Such a definition, I believe, could potentially leave out special districts that provide utility services, like the Salt River Project, the Central Arizona Project, the Metropolitan Water District of Southern California, and other smaller special districts.

My amendment, Madam Chair, which is supported by the American Public Power Association, changes the bill to read, ''political subdivision,'' allowing more utilities to receive the protections built into our bill. In doing so, it also makes the language consistent with the preemption provision in the bill.

If not amended, this legislation could subject utility districts to additional requirements if they share threat information, effectively creating a deterrent to participation—precisely what we want to avoid. We know that myriad threats are arrayed against the networks that run our critical infrastructure, and we must ensure that the utilities, which are the front lines in the cybersecurity fight, are properly protected.

I have long advocated for minimum standards for utilities, but absent such standards, I believe that we have to make sure that as many utilities as possible have access to the best possible information to defend their networks and are able to share information about the attacks that they experience.

This is an important bill overall. I really do want to applaud, again, Chairman ROGERS and Ranking Member RUPPERSBERGER for their outstanding work on the underlying bill.

Obviously, the challenges of the threats that we face in cyberspace are growing exponentially every day. It seems like there's not a week that goes by that you don't hear of a new major attack on the critical infrastructure or, in particular, our banking system or major corporations with intellectual property theft, and obviously we have got to take action and do so now. Failure to do so would be a great abdication of our responsibility.

I'm disappointed the bill didn't pass last year. I know how hard the chairman and ranking member worked on this legislation, but clearly our adversaries, or enemies, have not taken a hiatus. They are actively engaged in cyber attacks or threats of intellectual property or identity theft, and the list goes on and on.

The underlying bill is a major step forward in protecting our cyber networks, allowing classified information to be shared with the private sector, allowing threat information to be shared back with the government to give broader situation awareness, as well as information sharing between both in the private sector among companies.

So, again, the underlying bill is a major step forward. I believe this amendment that I'm offering makes the bill even better for making sure that broader utilities are included in allowing for information sharing.

I urge my colleagues to support this commonsense amendment and the underlying legislation, and I reserve the balance of my time.

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

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

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

I want to thank the gentleman from Rhode Island (Mr. LANGEVIN), who has been a tremendous leader on cybersecurity efforts on the Intelligence Committee. Much of our work there is classified and it goes unnoticed, and rightly so. I think it would be wrong for us not to commend in public your great leadership and efforts and work with us to try to make sure that this bill does what we say we want it to do. It has been a great privilege and pleasure to work with you throughout that process, and without that leadership, we wouldn't be standing on the floor today. I want to thank the gentleman for that.

I will support the amendment, which clarifies that entities located across multiple localities are intended to be covered by provisions in the bill exempting information shared under the bill from certain disclosures otherwise required of public or quasi-public entities. The amendment replaces the term ''local'' with ''political subdivision.'' Because there is no intention to exclude such entities, this is intended as a clarification, an important clarification, and I will gladly support the amendment, and again thank the gentleman for his work on the totality of both national security issues and cybersecurity.

I reserve the balance of my time.

Mr. LANGEVIN. Madam Chair, I yield such time as he may consume to the ranking member of the Intelligence Committee, the gentleman from Maryland (Mr. RUPPERSBERGER).

Mr. RUPPERSBERGER. I thank the gentleman for yielding.

Madam Chair, first, I want to agree with our chairman, and I said it before, that you have been one of the key players in developing legislation to protect our country. From the beginning, when those of us started working on this issue, probably 2006, you were there. You have a tremendous amount of expertise. You have been a great adviser to all of us, and also not only the Intelligence Committee, but the Armed Services Committee, and I appreciate all your work.

I also support your amendment to include political subdivisions within the information, use, and protection requirements in our bill. Your amendment ensures that utility districts are not unnecessarily and unintentionally limited from protecting their own information.

Therefore, I urge a ''yes'' vote on your amendment.

Mr. LANGEVIN. Madam Chair, before I close, I just wanted to thank, again, the chairman and the ranking member for their comments, but, more importantly, their extraordinary collaborative work in trying to protect our Nation's cybersecurity. The work that they did in putting this legislation together, it is a real service to the country what you have done, and I am grateful to have played a part in it with you, and thank you for your friendship.

With that, I urge my colleagues to support the amendment, and I yield back the balance of my time.

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

The CHAIR. The question is on the amendment offered by the gentleman from Rhode Island (Mr. LANGEVIN).

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

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

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

□ 1600

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

The motion was agreed to.

Accordingly, the Committee rose; and the Speaker pro tempore (Mr. MARCHANT) having assumed the chair, Ms. ROS-LEHTINEN, 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.

Accordingly (at 4 o'clock and 1 minute p.m.), the House stood in recess.

□ 1630

AFTER RECESS

The recess having expired, the House was called to order by the Speaker pro tempore (Mr. HARRIS) at 4 o'clock and 30 minutes p.m.

CYBER INTELLIGENCE SHARING AND PROTECTION ACT

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 Texas (Mr. MARCHANT) kindly take the chair.

□ 1631

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. MARCHANT (Acting Chair) in the chair.

The Clerk read the title of the bill.

The Acting CHAIR. When the Committee of the Whole rose earlier today, a request for a recorded vote on amendment No. 4 printed in House Report 113–41 offered by the gentleman from Rhode Island (Mr. LANGEVIN) had been postponed.

Pursuant to clause 6 of rule XVIII, proceedings will now resume on those amendments printed in House Report 113–41 on which further proceedings were postponed, in the following order:

Amendment No. 1 by Mr. ROGERS of Michigan.

Amendment No. 2 by Mr. CONNOLLY of Virginia.

Amendment No. 4 by Mr. LANGEVIN of Rhode Island.

The Chair will reduce to 2 minutes the minimum time for any electronic vote after the first vote in this series.

AMENDMENT NO. 1 OFFERED BY MR. ROGERS OF MICHIGAN

The Acting CHAIR. The unfinished business is the demand for a recorded vote on the amendment offered by the gentleman from Michigan (Mr. ROGERS) on which further proceedings were postponed and on which the ayes prevailed by voice vote.

The Clerk will redesignate the amendment.

The Clerk redesignated the amendment.

RECORDED VOTE

The Acting CHAIR. A recorded vote has been demanded.

A recorded vote was ordered.

The vote was taken by electronic device, and there were—ayes 418, noes 0, not voting 14, as follows:

[Roll No. 110]

AYES—418

Aderholt	Bucshon	Cook
Alexander	Burgess	Cooper
Amash	Bustos	Costa
Amodei	Butterfield	Cotton
Andrews	Calvert	Courtney
Bachus	Camp	Cramer
Barber	Campbell	Crawford
Barletta	Cantor	Crenshaw
Barr	Capito	Crowley
Barrow (GA)	Capps	Cuellar
Barton	Capuano	Culberson
Bass	Cárdenas	Cummings
Beatty	Carney	Daines
Becerra	Carson (IN)	Davis (CA)
Benishek	Carter	Davis, Danny
Bentivolio	Cartwright	Davis, Rodney
Bera (CA)	Cassidy	DeFazio
Bilirakis	Castor (FL)	DeGette
Bishop (GA)	Castro (TX)	Delaney
Bishop (NY)	Chabot	DeLauro
Bishop (UT)	Chaffetz	DelBene
Black	Chu	Denham
Blumenauer	Cicilline	Dent
Bonamici	Clarke	DeSantis
Bonner	Clay	DesJarlais
Boustany	Cleaver	Deutch
Brady (PA)	Clyburn	Diaz-Balart
Brady (TX)	Coble	Dingell
Braley (IA)	Coffman	Doggett
Bridenstine	Cohen	Doyle
Brooks (AL)	Cole	Duckworth
Brooks (IN)	Collins (GA)	Duffy
Broun (GA)	Collins (NY)	Duncan (SC)
Brown (FL)	Conaway	Duncan (TN)
Brownley (CA)	Connolly	Edwards
Buchanan	Conyers	Ellison