NOT VOTING—11

Davis (KY)	McHenry	Sullivan
Filner	Paul	Waters
Holden	Rangel	Waxman
Marino	Slaughter	

□ 1405

Mr. BILIRAKIS changed his vote from ''nay'' to ''yea.''

So the previous question was ordered.

The result of the vote was announced as above recorded.

Stated against:

Mr. FILNER. Madam Speaker, on rollcall 182, I was away from the Capitol due to prior commitments to my constituents. Had I been present, I would have voted "nay."

The SPEAKER pro tempore (Mrs. BIGGERT). The question is on the resolution.

The question was taken; and the Speaker pro tempore announced that the ayes appeared to have it.

Mr. POLIS. Madam Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. This will be a 5-minute vote.

The vote was taken by electronic device, and there were—yeas 236, nays 185, not voting 10, as follows:

[Roll No. 183]

YEAS—236

Adams	Duncan (SC)	Kelly
Aderholt	Duncan (TN)	King (IA)
Akin	Ellmers	King (NY)
Alexander	Emerson	Kingston
Amash	Farenthold	Kinzinger (IL)
Amodei	Fincher	Kline
Austria	Fitzpatrick	Labrador
Bachmann	Flake	Lamborn
Bachus	Fleischmann	Lance
Barletta	Fleming	Landry
Bartlett	Flores	Lankford
Barton (TX)	Forbes	Latham
Bass (NH)	Fortenberry	LaTourette
Benishek	Foxx	Latta
Berg	Franks (AZ)	Lewis (CA)
Biggert	Frelinghuysen	LoBiondo
Bilbray	Gallegly	Long
Bilirakis	Gardner	Lucas
Bishop (UT)	Garrett	Luetkemeyer
Black	Gerlach	Lummis
Blackburn	Gibbs	Lungren, Daniel E.
Bonner	Gibson	Mack
Bono Mack	Gingrey (GA)	Manzullo
Boustany	Gohmert	Marchant
Brady (TX)	Goodlatte	Matheson
Brooks	Gosar	McCarthy (CA)
Broun (GA)	Gowdy	McCaul
Buchanan	Granger	McClintock
Bucshon	Graves (GA)	McCotter
Buerkle	Graves (MO)	McKeon
Burgess	Griffin (AR)	McKinley
Burton (IN)	Griffith (VA)	McMorris Rodgers
Calvert	Grimm	Meehan
Camp	Guinta	Mica
Campbell	Guthrie	Miller (FL)
Canseco	Hall	Miller (MI)
Cantor	Hanna	Miller, Gary
Capito	Harper	Mulvaney
Carter	Harris	Murphy (PA)
Cassidy	Hartzler	Myrick
Chabot	Hastings (WA)	Neugebauer
Chaffetz	Hayworth	Noem
Coble	Heck	Nugent
Coffman (CO)	Hensarling	Nunes
Cole	Herger	Nunnelee
Conaway	Herrera Beutler	Olson
Cravaack	Huelskamp	Palazzo
Crawford	Huizenga (MI)	Paulsen
Crenshaw	Hultgren	Pearce
Culberson	Hunter	Pence
Denham	Hurt	Petri
Dent	Issa	Pitts
DesJarlais	Jenkins	Platts
Diaz-Balart	Johnson (IL)	Poe (TX)
Dold	Johnson (OH)	Pompeo
Dreier	Johnson, Sam	Posey
Duffy	Jordan	Price (GA)
Quayle	Ryan (WI)	Tiberi
Reed	Scalise	Tipton
Rehberg	Schilling	Turner (NY)
Reichert	Schmidt	Turner (OH)
Renacci	Schock	Upton
Ribble	Schweikert	Walberg
Rigell	Scott (SC)	Walden
Rivera	Scott, Austin	Walsh (IL)
Roby	Sensenbrenner	Webster
Roe (TN)	Shimkus	West
Rogers (AL)	Shuler	Westmoreland
Rogers (KY)	Shuster	Whitfield
Rogers (MI)	Simpson	Wilson (SC)
Rohrabacher	Smith (NE)	Wittman
Rokita	Smith (NJ)	Wolf
Rooney	Smith (TX)	Womack
Ros-Lehtinen	Southerland	Woodall
Roskam	Stearns	Yoder
Ross (FL)	Stivers	Young (AK)
Royce	Stutzman	Young (FL)
Runyan	Terry	Young (IN)
	Thompson (PA)	
	Thornberry	

NAYS—185

Ackerman	Frank (MA)	Napolitano
Altmire	Fudge	Neal
Andrews	Garamendi	Olver
Baca	Gonzalez	Owens
Baldwin	Green, Al	Pallone
Barrow	Green, Gene	Pascrell
Bass (CA)	Grijalva	Pastor (AZ)
Becerra	Gutierrez	Pelosi
Berkley	Hahn	Perlmutter
Berman	Hanabusa	Peters
Bishop (GA)	Hastings (FL)	Peterson
Bishop (NY)	Heinrich	Pingree (ME)
Blumenauer	Higgins	Polis
Bonamici	Himes	Price (NC)
Boren	Hinchey	Quigley
Boswell	Hinojosa	Rahall
Brady (PA)	Hirono	Reyes
Braley (IA)	Hochul	Richardson
Brown (FL)	Holt	Richmond
Butterfield	Honda	Ross (AR)
Capps	Hoyer	Rothman (NJ)
Capuano	Israel	Roybal-Allard
Cardoza	Jackson (IL)	Ruppersberger
Carnahan	Jackson Lee (TX)	Rush
Carney	Johnson (GA)	Ryan (OH)
Carson (IN)	Johnson, E. B.	Sánchez, Linda T.
Castor (FL)	Jones	Sanchez, Loretta
Chandler	Kaptur	Sarbanes
Chu	Keating	Schakowsky
Cicilline	Kildee	Schiff
Clarke (MI)	Kind	Schrader
Clarke (NY)	Kissell	Schwartz
Clay	Kucinich	Scott (VA)
Cleaver	Langevin	Scott, David
Clyburn	Larsen (WA)	Serrano
Cohen	Larson (CT)	Sewell
Connolly (VA)	Lee (CA)	Sherman
Conyers	Levin	Sires
Cooper	Lewis (GA)	Smith (WA)
Costa	Lipinski	Speier
Costello	Loebsack	Stark
Courtney	Lofgren, Zoe	Sutton
Critz	Lowey	Thompson (CA)
Crowley	Luján	Thompson (MS)
Cuellar	Lynch	Tierney
Cummings	Maloney	Tonko
Davis (CA)	Markey	Towns
Davis (IL)	Matsui	Tsongas
DeFazio	McCarthy (NY)	Van Hollen
DeGette	McCollum	Velázquez
DeLauro	McDermott	Visclosky
Deutch	McGovern	Walz (MN)
Dicks	McIntyre	Wasserman Schultz
Dingell	McNerney	Waters
Doggett	Meeks	Watt
Donnelly (IN)	Michaud	Waxman
Doyle	Miller (NC)	Welch
Edwards	Miller, George	Wilson (FL)
Ellison	Moore	Woolsey
Engel	Moran	Yarmuth
Eshoo	Murphy (CT)	
Farr	Nadler	
Fattah		

NOT VOTING—10

Davis (KY)	McHenry	Slaughter
Filner	Paul	Sullivan
Holden	Rangel	
Marino	Sessions	

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore (during the vote). There are 2 minutes remaining.

□ 1414

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.

Stated against:

Mr. FILNER. Madam Speaker, on rollcall No. 183, I was away from the Capitol due to prior commitments to my constituents. Had I been present, I would have voted "nay."

LOWELL NATIONAL HISTORICAL PARK LAND EXCHANGE ACT OF 2012

The SPEAKER pro tempore. The unfinished business is the question on suspending the rules and passing the bill (H.R. 2240) to authorize the exchange of land or interest in land between Lowell National Historical Park and the city of Lowell in the Commonwealth of Massachusetts, and for other purposes, as amended.

The Clerk read the title of the bill.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Utah (Mr. BISHOP) that the House suspend the rules and pass the bill, as amended.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

□ 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 in which to revise and extend their remarks and include extraneous material on H.R. 3523.

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

There was no objection.

The SPEAKER pro tempore. Pursuant to House Resolution 631 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. 3523.

The Chair appoints the gentlewoman from Illinois (Mrs. BIGGERT) 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. 3523) 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 Mrs. BIGGERT 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. Madam Chair, I yield myself 4 minutes.

Never a problem have I seen when it comes to our national security, Madam Chair, that we are just not prepared to handle.

In just the last few years, nation-states, like China, have stolen enough intellectual property from just the Fed's contractors that it would be equivalent to 50 times the print collection of the Library of Congress. We have nation-states that are literally stealing jobs and our future. We also have countries that are engaged in activities and have capabilities that have the ability to break networks, computer networks, which means you can't just reboot. It means your system is literally broken. Those kinds of disruptions can be catastrophic when you think about the financial sector or the energy sector or our command and control elements for all of our national security apparatus.

This is as serious a problem as I have seen. So, last year, I and my partner—DUTCH RUPPERSBERGER, the vice chairman and ranking member of the Intelligence Committee—agreed that this was a significant enough problem to the future prosperity of America that we'd better do something about it.

We needed to stop the Chinese Government from stealing our stuff. We needed to stop the Russians from what they're doing to our networks and to people's personal information, data, and resources. We needed to prepare for countries like Iran and North Korea so that they don't do something catastrophic to our networks here in America and cause real harm to real people.

So, in a bipartisan way, we set out to do something very, very, very narrow. When the government spies overseas, it collects malware—viruses, software that is dangerous to our computers. That means they can either steal our stuff—the personal information off of your computer—or they can steal the secrets that make your business viable, the kinds of secrets that give people jobs.

So wouldn't it be great if we could take that source code, that software and share it with the private sector so that they could put it on their private systems, like they do every single day to try to protect networks, and have that added advantage of that extra coverage from that malicious source code? The good news is this happens every day. If you have Norton or McAfee or Symantec or any other antivirus protection on your computer, it has patches of information that they know is really bad stuff, and every time you turn your computer on, it updates and tries to protect your computer, your personal information.

That's all this is. It is adding to that patchwork some zeroes and some ones that we know is malicious code that is either going to steal your information or break your computer or something worse. That's all this bill is. It draws a very fine line between the government and the private sector. It is all voluntary. There are no new mandates. There is no government surveillance—none, not any—in this bill. It just says, if we know we have this source code, shouldn't we be obligated to give it so it doesn't do something bad to the companies and individuals in America. That's all this bill does.

We have worked collaboratively with hundreds of companies, with privacy groups, with civil libertarians. We have worked with government folks. We have had hundreds and hundreds of meetings for over a year. We have kept this bill open in an unprecedented transparent way to try to meet the needs of privacy concerns, civil libertarian concerns, civil liberties concerns. We wanted to make sure that, with this bill, people understood exactly what we were trying to do, how simple it is, and how crucial it is to the future defense of this great Nation.

Without our ideas, without our innovation that countries like China are stealing every single day, we will cease to be a great Nation. They are slowly and silently and quickly stealing the value and prosperity of America.

The CHAIR. The time of the gentleman has expired.

Mr. ROGERS of Michigan. I yield myself an additional 1 minute.

One credit card company said that they get attacked for your personal information 300,000 times a day—one company. We have a company that can directly show you stolen intellectual property. This one particular company estimated 20,000 manufacturing jobs that they lost for Americans, which were good-paying jobs, because countries like China stole their intellectual property and illegally competed against them in the marketplace.

This is as bad a problem, Madam Chair, as I have seen. I think you'll hear throughout the day this has been a responsible debate and that it has been a responsible negotiation to get to privacy concerns and our ability to protect your information on your computer through this series of zeroes and ones, the binary code on our computers.

Again, I want to thank my ranking member for his partnership and his work. He has been exceptional to work with on something on which we both agree and on which we agreed, in a bipartisan fashion, was a danger to the future prosperity of America.

With that, I reserve the balance of my time.

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

First of all, I do want to thank the chairman for working with us in a bipartisan way to protect our country from this very serious threat of cyberattacks.

As the ranking member of the House Intelligence Committee, people often ask me what keeps me up at night. I tell them: weapons of mass destruction entering the country undetected and also a catastrophic cyberattack shutting down our water supply, power grid or banking systems; and those are just a few of the many areas that could be attacked and shut down.

Every day, U.S. Web sites and our Nation's networks are threatened by foreign governments like China, Iran, Russia, and other groups trying to steal our money and valuable trade secrets. According to the National Counterterrorism Executive, the number one thing cyberthieves are trying to steal is information and communication technology, which form the backbone of nearly every other technology. In fact, according to the United States Cyber Command, $300 billion worth of trade secrets are stolen every year. This proves we need to make real changes to how we protect our cybersystems.

The Cyber Intelligence Sharing and Protection Act helps the private sector protect itself and its clients from these attackers and data thieves. The intelligence community has the ability to detect these cyberthreats, these malicious codes and viruses, before they are able to attack our networks; but right now, Federal law prohibits the intelligence community from sharing the classified cyberthreat with the companies that will protect us, that control the network—the AT&Ts, the Verizons, the Comcasts, those groups. We have the ability to give them the information to protect us; yet we have to pass a law to do that, and that's why we are here today.

□ 1430

The Cyber Intelligence Sharing and Protection Act will clearly do that if we pass the bill. It allows the intelligence community to share the codes and signatures associated with malware and viruses and the means to counter the bad stuff with the companies. These companies keep a lookout for these viruses and work to stop them before they are able to attack their system.

Companies then voluntarily give information about the cyberattack back to the government, machine code consisting of strings of zeroes and ones that uniquely identifies the malware. Cyberanalysts will use this information to better understand the attack and try to figure out who launched it and where it came from.

This information will be used to protect against similar attacks in the future.

Now, the Democrats worked hard to protect privacy and civil liberties in this bill throughout the entire process. We fought for additional privacy protections in the original bill that was marked up in committee. In the version we will vote on tomorrow morning, additional changes are also included in the amendments.

Privacy and civil liberty groups and the White House all agree we made important positive changes that went a long way to improve the initial bill that came out of committee. We severely limit what information can be shared with the government and how it can be used.

It is also important to note the entire process is completely voluntary and provides industry the flexibility they need to deal with business realities.

The bill also requires an annual report from the inspector general of the intelligence community to ensure none of the information provided to the government is mishandled or is misused. This is a very important privacy issue.

The review will include annual recommendations to improve the protection of privacy and civil liberties. That review will be done again by the inspector general.

We also made it clear this legislation grants no new authority to the Department of Defense, the National Security Agency, or the intelligence community. At the urging of the White House and others, we included the Department of Homeland Security in the process so that there is not even a perception that our intelligence agencies or military will be in control of this. The Homeland Security Department will be coordinating as a civil body.

In addition, companies that act in good faith to protect systems and networks can receive liability protection. This is what our bill does.

Now, what does it not do? The bill does not allow the government to order companies to turn over private email or other personal information. This is not surveillance. The bill does not allow the government to monitor private networks, read private email, censor, or shut down any Web site.

We have a broad coalition of support with 100 cosponsors, close to 30 companies and industry groups, and dozens of trade organizations like Facebook, Microsoft, IBM, a lot of different groups that are supporting this bill.

This is not a perfect bill, but the threat is great. I believe this legislation is critical for our national security and yet deals with the issue of privacy. We can do better in privacy, and we hope to get the bill to the Senate, where there will be a lot more negotiation. Congress must act now, and I encourage my colleagues to vote for this bill.

I reserve the balance of my time.

Mr. ROGERS of Michigan. I yield 2 minutes to the gentlelady from North Carolina (Mrs. MYRICK) who is on the Intelligence Committee and has a tremendous expertise on counterterrorism issues.

Mrs. MYRICK. I want to say a big thanks to the chair and to the ranking member for all of their months of hard work on putting this cybersecurity bill together, and it is a bipartisan Intelligence Committee bill.

We all know the private sector is a very diverse world that includes reputable companies but also grey market suppliers and counterfeiters, and State-owned enterprises and other entities that often act against the national security interests of the United States, as well as other private companies.

The information technology sector, in particular, includes companies that are associated with some foreign governments and militaries and intelligence services of nations that attack the United States in cyberspace daily.

State and local entities, along with the private sector, don't have the resources, the capabilities, or the information necessary to address these cybersecurity threats. This bill creates a necessary mechanism for the Federal Government to share its informational resources and cybersecurity threat analysis with the private sector and with State and local entities.

The purpose of the bill is to transmit important cybersecurity information from the Federal Government to the private sector, not vice versa. The bill would empower the private sector to begin taking necessary steps to protect itself from cyberattacks, some they don't have any clue are happening.

Ultimately though, it's going to be important for Congress and the Federal Government to continue the debate on cybersecurity to determine how to best confront the changing threats because this world is changing daily, and the Federal Government can't leave those responsibilities solely to the private sector, especially, like the chairman already mentioned, countries like China that are continuously developing cyberwarfare capabilities and the cyberattacks that they commit against the Western companies and infrastructures and government entities we all know about.

So I urge my colleagues to vote ''yes'' on this important piece of legislation and an important step in trying to protect the private sector in this country.

Mr. RUPPERSBERGER. Madam Speaker, I yield 2 minutes to my distinguished colleague from the State of Utah (Mr. BOSWELL) who formerly served on the Intelligence Committee.

The CHAIR. The gentleman from Iowa is recognized for 2 minutes.

Mr. BOSWELL. Thank you, I appreciate the correction. We grow corn in Iowa, and we grow potatoes in Idaho. A little bit of fun.

I rise to speak in support of this bill today. I look across at Chairman ROGERS and here at Ranking Member RUPPERSBERGER, and I have great confidence. I know these men. I know their staff. They've come to this very serious matter that lays before our country that we need to understand. We must take action.

I'm encouraged by the process to involve key stakeholders from private industry and privacy groups during this drafting. This transparent engagement shaped many of the bipartisan constructive amendments being considered today that will improve the bill, and it's a good thing.

The threat from malicious actors in cyberspace is real. You've heard it said over and over already by those who have spoken ahead of me. I concur with what they say. It's an absolutely real thing. You only need to pick up the newspaper or turn on the TV to see the threats facing our networks. These networks include those that power our homes, our factories, and our small businesses, allow our banking system to function and provide the very backbone to our current American way of life, and we rely on these networks every day.

The bill under consideration today is a very narrow piece, but what we can agree on is it's a critical one to helping secure our networks and, therefore, the way of life as we know it today.

There are continuing debates on how to implement the bill, but the debate isn't over what needs to be done; it must be done. Information we ask our intelligence community to use and that protects our government networks should, in a secure way, be shared to protect the many other critical networks we rely on.

I believe companies are doing what they can to protect their networks to the extent they can today, but there is more that must be done.

We cannot be in a situation where the government had information to prevent or mitigate a catastrophic cyberattack, and yet we did not have the procedure in place to share this information. Our American way of life includes a great respect for privacy and our civil liberties. We make no mistake about that.

This bill, with the addition of many of the amendments which were drafted in concert with privacy groups, addresses many of those concerns.

In addition, the annual unclassified report required by the statutory intelligence community inspector general will inform whether there are additional adjustments needed to be made.

The CHAIR. The time of the gentleman has expired.

Mr. RUPPERSBERGER. I yield the gentleman an additional 10 seconds.

Mr. BOSWELL. So, in closing, I want to say this: Congress cannot wait to act. Network security hasn't kept up with network speed. This is the fundamental purpose of this bill. I encourage Members to begin to secure our networks through sharing information about the threats. Please vote ''yes.''

Mr. ROGERS of Michigan. I yield 2 minutes to the gentleman from Illinois (Mr. KINZINGER).

Mr. KINZINGER of Illinois. I thank the ranking member and the chairman for your hard work on the issue and the members on the committee.

This is very important. It goes beyond partisanship. This is about national security.

The idea of cyberattacks, it's not something that is just out there in space that we really don't have to worry about. This is an issue that's here today, and it's here right now. In

fact, just today, the New York Stock Exchange was the target of a DDoS attack on some of its external computer systems. That's not something that we just magically happen to have today. This is happening every day, thousands and thousands of times a day.

□ 1440

I'm a military guy and I'm a military pilot. I think a lot about the threats from outside. You think a lot about threats of terrorism and threats of invasion or anything along that line. But I'll tell you one of the biggest threats that really keep us up at night is this idea of a cyberattack. I think it's something that we have to take head-on. This voluntary information-sharing between classified portions of our government and certified private actors will serve to enhance our defenses greatly.

It is important to note the amount of classified information currently shared between our government and private industry is muddled at best. The few private companies who are lucky enough to receive an invitation into the current classified annex of cybersecurity-sharing face significant challenges when it comes to even understanding what that information is. Many times they simply get a badly scanned printout of a current threat situation from which they try to prevent a future attack, and it is woefully inadequate.

We talk a lot about the Russians and about the Chinese and their use of cyberwarfare against us. That's a significant threat. That's something very serious. But I want to speak just momentarily about the threat from Iran.

We all know that Iran is a very serious country that is very seriously focused on bringing down, in many cases, the West. They've said it themselves. The Iranian regime from the highest level down has publicly stated their plans to fight enemies with abundant power in cyberspace and Internet warfare. It's also publicly stated that Iran blames the West for the Stuxnet virus which disrupted their nuclear program, and they have vowed retaliation. The combination of the low cost and effectiveness of cyberwarfare has led the Iranian Revolutionary Guard to actively and effectively recruit radical Islamist hackers for nefarious purposes. We can't stand idly by while we see nations like Iran threaten the future of this country.

So I support this bill, and I commend the folks who have worked on it.

Mr. RUPPERSBERGER. Madam Chair, I yield 2 minutes to my distinguished colleague from the State of New Jersey, Mr. RUSH HOLT, who was formally on the Intelligence Committee.

Mr. HOLT. Madam Chair, I thank the gentleman.

The proponents of this legislation, who are all friends and well intentioned, have repeatedly said there's a real threat, a threat to our critical infrastructure, affecting our waterworks, and our electric grid. But this bill is so poorly constructed it is not designed to protect against those threats. There are any number of flaws with it.

The American Civil Liberties Union points out that there would be an exception to all privacy laws; and it would allow companies to share private and personal data that they hold on their American customers, actually, among themselves and with the government. It would not limit companies to sharing only technical or nonpersonal data. They'd be free from any liability of misuse. They would only have to plead good intentions.

The bill fails to narrowly define the privacy laws it would contravene; it fails to put the cybersecurity efforts in a civilian agency; it fails to require companies to remove personal identifiable information about individuals; it fails to sufficiently limit the government's use of information; it fails to create a robust oversight and accountability structure. With the bill in its current form, there's no requirement that personal information must be removed. There's no consumer or stakeholder group involved in the oversight. There's no way for any member of the public to know if their data has been shared in error, and on and on.

And I should point out that it is not just the American Civil Liberties Union that opposes this. Even the American Library Association opposes it. The President, himself, says, if this passes, he will veto it. Passing this bill in response to the cyberthreat would be like going into Iraq because al Qaeda terrorists were a real threat.

Yes, there's a real threat. This is not the answer.

Mr. ROGERS of Michigan. Madam Chair, I yield 2 minutes to the distinguished gentleman from Ohio (Mr. STIVERS).

Mr. STIVERS. Madam Chair, I would like to thank the gentleman from Michigan for yielding me time. I would also like to thank him for his leadership on this effort, as well as the ranking member, the gentleman from Maryland (Mr. RUPPERSBERGER).

I rise today in support of the cybersecurity legislation under consideration. As a member of the Cybersecurity Task Force, I'm pleased that many of our recommendations are included in this bill.

Cybersecurity is a very important issue. Every day there are people trying to use cyberattacks to steal our money, steal our jobs, and attack our national security.

I know as a member of the Financial Services Committee that our financial sector spends billions of dollars every year trying to protect against cyberattacks. They protect consumers by increasing controls, making sure they have encryption, authenticating customers, and protecting customer data.

That's all protecting our wallets, but we also need to protect our jobs. Unfortunately, there are folks who would like to use cyberattacks to steal our intellectual property and give it to those who compete against America, which will steal our jobs.

Not allowing information-sharing like this bill does would be like saying to the Marines and the Army, You can't share information about how the enemy is going to attack you. As a member of the National Guard for the last 26 years, I know that cyber is also a real threat to our national security.

This bill will update our information-sharing to allow private companies to share information with the government and the government to share information, and includes some important liability protection as well. It's a carefully crafted bill.

I think the gentleman from Michigan (Mr. ROGERS) and the gentleman from Maryland (Mr. RUPPERSBERGER) have been very open to working with folks to try to improve this bill. I'm looking forward to supporting some of the bipartisan amendments that I think will improve this bill.

Madam Chair, we must protect ourselves against cyberattacks, against those who would steal our money, steal our jobs, and attack our country. This bill is not a panacea, but it's a great start. I'm happy to support it, and I hope all my colleagues will vote ''yes.''

Mr. RUPPERSBERGER. I yield 2 minutes to my distinguished colleague from the State of California, Mr. ADAM SCHIFF, who is also the ranking member on the Technical and Tactical Intelligence Committee.

Mr. SCHIFF. I thank the gentleman for yielding.

Madam Chair, I rise in reluctant opposition to the bill. But at the outset, I want to acknowledge the extraordinary work done by our chairman, MIKE ROGERS, and our ranking member, DUTCH RUPPERSBERGER. These two gentlemen have changed the nature and culture of our committee, made it far more productive, and they've done great work getting us to this point. And I want to acknowledge that at the outset.

There's still work to be done in two areas principally, and I want to talk briefly about that. Even before I do that, I want to acknowledge why we're here.

We do ourselves, I think, a disservice when we talk about a cyberthreat. That sounds like something that may come in the future, something to be concerned about that might take place down the line. We're under cyberattack right now. This is not speculative. This is not intangible. This is happening right now. This needs to be dealt with, and we do need a sense of urgency. But there is a distance yet to go, and in two areas in particular.

One is, when we gather cyberinformation and we share it between companies or between the government and companies, as we must do, we want to make sure that we minimize any unnecessary invasion of privacy of the American people. We can

do both, and we have to do both. We need to protect ourselves from cyberattack, and we need to protect and preserve the privacy rights of the American people.

I think the bill needs a requirement that personally identifiable information be minimized to the maximum extent practicable. All we're asking for is what can reasonably be done. We're not asking for the private sector or the government to do the impossible, but we should require of our government that they minimize personal information that is shared to protect us from cybercrime. That's the first thing.

The second item that really needs to be incorporated in this bill that my colleague, Mr. THOMPSON, will talk about as well is the need to protect critical infrastructure. That is a big missing piece in the bill, and I understand from my colleagues that it's not within the Intelligence Committee jurisdiction. That's correct. But as we saw from the Rules Committee, they're more than capable of incorporating things from more than one committee's jurisdiction in the rule, as we see in a rule that incorporates student loan interest and a bill on that subject with a bill on cybersecurity. There is nothing preventing the Rules Committee from bringing into the discussion today and allowing amendments on critical infrastructure.

The absence of those two big pieces makes it impossible for me to support the bill today.

The CHAIR. The time of the gentleman has expired.

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

Mr. SCHIFF. I thank the gentleman.

I just want to conclude by saying I look forward to our continued work on this bill, and I appreciate the great cooperation between the chair and ranking member, and I have respect for all the members of the committee.

□ 1450

Mr. ROGERS of Michigan. Madam Chair, I yield 2 minutes to the gentleman from Nevada (Mr. HECK).

Mr. HECK. I come to the floor today to voice my strong support for the Cyber Intelligence Sharing and Protection Act. We know that every day, American companies and computer systems are targeted by foreign nation-state actors who prey on sensitive business and personal information to gain an unfair advantage in the global marketplace. The theft of research and development results, negotiating positions, or pricing information costs us jobs here at home and puts personal information at risk. The same vulnerabilities that can result in the theft of sensitive business information could be used to attack critical infrastructure we rely on such as power plants, air traffic control systems, and electrical grids. An attack on these systems would be devastating. Protecting them and the constituents they serve must be considered an urgent national security concern.

The government currently uses classified cyberthreat intelligence to protect its own systems, computer networks, and critical infrastructure. The business community has voiced its desire to be given the tools necessary to protect itself from cyberthreats. This bill will allow the government to provide classified cyberthreat information to private sector companies so that they can protect sensitive information and their customers' privacy against malicious cyberattacks. The bill places no mandates or burdens on private sector companies and does not expand the size or scope of the Federal Government. All information-sharing is totally voluntary under this legislation, and there are strong privacy protections in place for the information that is shared.

After receiving input from the private sector and civil liberty groups and by building upon the success of an existing intelligence-sharing pilot program with defense contractors, we have produced a bill that upholds constitutional rights to privacy while providing the private sector with the necessary means to defend itself against cyberattackers. I want to commend Chairman ROGERS and Ranking Member RUPPERSBERGER for their outstanding leadership in crafting this legislation that was written in a transparent and bipartisan fashion.

I urge my colleagues to support this bill that protects our homeland, protects our economy, and protects our privacy.

Mr. RUPPERSBERGER. Madam Chair, I yield 2 minutes to my distinguished colleague from the State of Mississippi, Mr. BENNIE THOMPSON, who is also the ranking member of the Homeland Security Committee.

Mr. THOMPSON of Mississippi. Madam Chairman, I rise in opposition to H.R. 3523. I also appreciate the efforts of my colleagues on the Intelligence Committee for fostering a greater sharing of cyberthreat information. This bill is a start, but my opposition is because it does not do what we know that we need to have done.

Having been involved in homeland security issues for nearly a decade, I know how important it is to protect our Nation's networks from cyberattacks. But in an effort to foster information-sharing, this bill would erode the privacy protections of every single American using the Internet. It would create a Wild West of information-sharing, where any certified business can share with any government agency, who can then use the information for any ''national security'' purpose and grant that business immunity from virtually any liability. None of the amendments offered by the chairman and ranking member would change any of those basic facts.

I and several of my colleagues offered amendments that would have addressed those concerns by ensuring that civilian agencies would take the lead in information-sharing, restricting how the government could use the information, and making sure consumers' sensitive information is adequately protected. Unfortunately, the House will not have an opportunity to consider them today.

If my colleagues want to accomplish something on cybersecurity, then vote ''yes'' on any or all of the suspension bills before us today; but do not vote for H.R. 3523. It violates the ''do no harm'' rule and would set back the privacy rights of all our citizens who have enjoyed the establishment of the Internet.

This fatally flawed bill is opposed by not only every major privacy or civil liberties group, from the ACLU to the Constitution Project to the Center for Democracy and Technology, but also the Obama administration. For these reasons, Madam Chair, I strongly urge a ''no'' vote on H.R. 3523.

Mr. ROGERS of Michigan. Madam Chair, I yield 2 minutes to the gentleman from Nebraska (Mr. TERRY).

Mr. TERRY. I thank the gentleman.

Madam Chairman, I rise in support of this bill. It's a sensible bill that builds a necessary pillar in the cybersecurity strategy of our Nation.

I've immersed myself in cybersecurity over the last couple of years. I've been on two task forces. I'm on the Energy and Commerce Committee. I've met with industry leaders in all of the critical infrastructure areas. And as I've gathered information and input, there's two principles at stake here. The common thread from all of them have said: we have to be flexible, and we have to be able to communicate. Those are the two principles on which this bill is based.

Number one, flexibility. What it means is you can't lock this into a government agency because when government agencies start taking control of setting standards or working with an industry group to set standards on cybersecurity, the hackers take 5 seconds to get around that, and it will take years then for the industry to move around that. You are setting them up as ducks waiting to be shot if we do that. So we can't. We've got to give them the flexibility. The least government interference is what gives them the flexibility.

The next part is communication. What I learned from the critical infrastructure industries is that what they want to know is, is there a threat out there, and what's the specifics of the threat? They know they're under attack every day. Maybe our defense agencies have specific information they can share, but they can't because it's top secret.

So this bill allows there to be communication of specific threats to perhaps communicate from government to private sector some better practices that they can enact. That's what this breaks down, that barrier, not some of these civil liberty conspiracy theories. This is simple communication between government and private sector or private sector to private sector. This isn't

reporting on whether you're downloading an illegal movie or whatever. This is about securing our infrastructure.

Mr. RUPPERSBERGER. Madam Chair, I yield 2 minutes to my distinguished colleague and friend from the State of Rhode Island (Mr. LANGEVIN), who is also a member of our Intelligence Committee and has worked very hard with the chairman and myself on the issue of cybersecurity. I consider him one of our experts on the Hill in the area of cybersecurity.

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

Mr. LANGEVIN. I want to thank the gentleman for yielding.

I rise in strong support of H.R. 3523, and I want to thank Chairman ROGERS and Ranking Member RUPPERSBERGER for a bipartisan and inclusive process on an extremely difficult and technical issue. While I don't believe this legislation is perfect, and much work remains to be done, CISPA represents an important good-faith effort to come together as a necessary first step towards better cybersecurity for our Nation.

I have long worked on this issue for many years to raise awareness and to secure our Nation against the threats that we face in cyberspace. Quite frankly, we are running out of time. I believe it's important that we act now to begin our legislative response to this critical issue.

We all know how dependent we are on the Internet and how we use it so much in our daily lives, but the Internet was never built with security in mind. What's happening is our adversaries are using the vulnerabilities against us.

I've also been very clear that we need to have robust privacy protections that must be included to safeguard personal information and also defend civil liberties in any cybersecurity response that we do enact. I'm pleased to say this legislation has been strengthened in that regard, and I believe more can be done as we continue this important debate.

That being said, the efficient sharing of cyberthreat information envisioned by this legislation is vital to combating advanced cyberthreats and stemming the massive ongoing theft of identities, intellectual property, and sensitive security information.

□ 1500

This legislation clearly and simply will allow the government to provide classified information threat signatures to the private sector and also allow the private sector to share with us the cybersecurity attacks that they are experiencing, sharing that with the government so we have better situational awareness. If you look at this, it basically gives us radar, if you will, in cyberspace, sharing information back and forth on cyberthreats that are facing the country.

This bill is a good step, but it's only a first step. Voluntary information-sharing is helpful and it's needed, but it does not, on its own, constitute strong cybersecurity.

The CHAIR. The time of the gentleman has expired.

Mr. RUPPERSBERGER. I yield the gentleman from Rhode Island 30 additional seconds.

Mr. LANGEVIN. I thank the gentleman for the additional time.

I have long maintained that we must also move forward on legislation that establishes minimum standards for the cybersystems that govern our critical infrastructure, particularly the electric grid and our water systems.

With that, I again want to thank Chairman ROGERS and Mr. RUPPERSBERGER for their outstanding efforts, and I ask my colleagues to support this important cybersecurity information-sharing legislation.

Mr. ROGERS of Michigan. Madam Chair, I yield 2 minutes to the gentlewoman from California (Mrs. BONO MACK).

Mrs. BONO MACK. Madam Chair, I rise today in strong support of this bill. This critically needed legislation will help to safeguard America in the future from cyberattacks by unscrupulous and rogue nations, terrorists and cybercriminals. We need to act before a disaster takes place, not after it, and this is our chance.

As chairwoman of the House Subcommittee on Commerce, Manufacturing and Trade, I have spent the past 16 months holding hearings and thoroughly examining the issue of online privacy. So as a cosponsor of this legislation, I have very carefully reviewed its privacy provisions, and I'm satisfied that it will not negatively impact American consumers.

Frankly, the privacy concerns are exaggerated. There is no bogeyman hiding in the closet, and Big Brother is not tapping into your hard drive. This bill provides absolutely no authority to the Federal Government to monitor private networks—none. Additionally, all information-sharing with the government would be completely voluntary.

The bill also encourages the private sector to ''anonymize'' the information it shares with the government or other entities, including—and this is very important to remember—the removal of personally identifiable information prior to sharing it.

Finally, the bill also requires the intelligence community inspector general to review information-sharing between the private sector and the government and to provide an annual report to the Congress on its findings.

These are very strong privacy protection features, and I applaud Chairman ROGERS and Ranking Member RUPPERSBERGER for working so hard to protect the American consumer and to make this a truly bipartisan effort.

Unfortunately, some people and some groups will say anything to try and scuttle this bill—sounding false alarms and raising imaginary red flags—despite the very real and dangerous threat posed by terrorists and our enemies if we do nothing.

Madam Chair, I strongly urge the adoption of H.R. 3523.

Mr. RUPPERSBERGER. I yield 2 minutes to my distinguished colleague from the State of Georgia (Mr. JOHNSON).

Mr. JOHNSON of Georgia. Thank you, Ranking Member RUPPERSBERGER.

Madam Chair, I rise in opposition to this very disturbing bill.

One thing that is important to keeping our country number one has been the personal freedoms that we have all enjoyed since this country's beginning. Those freedoms lie in the Bill of Rights. And the Fourth Amendment to the United States Constitution within that Bill of Rights provides for a right of privacy. Now this right of privacy can be impacted by technology and various advances in science that make eavesdropping, surveillance, and investigation easier and also more secretive by law enforcement, by personal individuals, and by corporations, by any component that may look to misuse information for their personal benefit. So I rise in opposition to this disturbing bill.

CISPA would grant the private sector blanket permission to harvest Americans' data for extremely broad ''cybersecurity purposes,'' notwithstanding any other provision of law. It would grant the private sector blanket permission to then share that data with the Federal Government, notwithstanding any other privacy laws or agreements with users.

The Acting CHAIR (Mrs. CAPITO). The time of the gentleman has expired.

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

Mr. JOHNSON of Georgia. Then, as if that weren't disturbing enough, this bill would grant the government broad authority to share that information between intelligence and law enforcement agencies and use it for virtually any purpose defined as important to cybersecurity or national security.

I know it's 2012, but it sure feels like ''1984'' in this House today. If you value liberty, privacy, and the Constitution, then you will vote ''no'' on CISPA.

Mr. ROGERS of Michigan. Madam Chair, I yield 2 minutes to the gentleman from California (Mr. NUNES).

Mr. NUNES. Madam Chair, I rise in strong support of this bill.

The bill before us today is targeted towards a very specific and growing threat to our Nation. Every day, American businesses are being targeted by China, Russia, and other foreign actors for cyber-exploitation and theft. These acts of industrial espionage are causing enormous losses of valuable American intellectual property that ultimately costs the United States jobs. We cannot afford to allow high-paying jobs to be stolen in this manner, nor can we simply sit by and allow the cyberwarfare being conducted against us to continue without consequences.

Madam Chairman, jobs are at stake, as is the technological capital of the United States. But if the reality of this economic cyberwarfare isn't convincing enough, you should understand that there are other good reasons for us to support this bill.

The state-of-the-art technology stolen from Americans can easily be turned against us and represents a serious threat to America's critical infrastructure. None in this body would likely disagree that we have to prevent our enemies from protecting American military technology. That's why we have long had export controls and other mechanisms to prevent such a thing from occurring. Madam Chairman, how is the theft of intellectual property any less a threat today?

Whether we like it or not, cyberwarfare is a reality. Our government and its security agencies understand this and are using both classified and unclassified information to fight the threat. But without passage of this bill, they are being forced to do so without the meaningful participation of industries—private industries—that are being subjected to attacks, that in some cases our government even knows about but cannot share that with those private companies.

So we shouldn't expect America's private sector innovators to protect themselves if we won't tell them where the attacks are coming from. If we don't share this information or allow them to share information with us, how do we expect to secure the sensitive information?

The Acting CHAIR. The time of the gentleman has expired.

Mr. ROGERS of Michigan. I yield the gentleman from California an additional 30 seconds.

Mr. NUNES. So we essentially have three choices. We can pass this bill, very narrowly focused, allowing our intelligence community to work with private industry, or we can fund a massive new government program. I think we've proven that those massive new government programs seldom work and are often costly. Or would the opponents of this bill simply rather do nothing and allow our country to continue to be attacked every day?

We need to pass this bill to enable cyberthreat-sharing and provide clear authority for the private sector to defend its networks.

Madam Chair, I want to close by saying that we should congratulate Chairman ROGERS and Ranking Member RUPPERSBERGER for the work that they've done to protect this country.

□ 1510

Mr. RUPPERSBERGER. Madam Chair, I yield 3 minutes to my distinguished colleague from the State of Oklahoma (Mr. BOREN), who is also a member of the Intelligence Committee. He has worked very closely with me and the chairman to bring this bill to the floor today, and we thank him for that.

Mr. BOREN. Madam Chair, I rise today in support of the Cyber Intelligence Sharing and Protection Act. I'm proud to have been a part of this bipartisan effort, led by Chairman ROGERS and Ranking Member RUPPERSBERGER, to bring this bill to the floor today.

There is one fact on which everyone can agree: our country must strengthen its cybersecurity capabilities. To achieve this, we need the cooperation of industry, government, and our citizens, and we need to protect the unique interests of each of these groups.

Some may be asking the question, how does this bill protect American industry? It gives private companies the ability to receive classified information from the government to protect their networks. The bill also gives them flexibility to share information with the government without compromising their business equities or harming their customers. This information-sharing partnership will enhance government efforts to analyze and understand malicious codes and other cyberthreats.

I think companies that have publicly supported this legislation have gotten a bad rap in the press. I think we all need to remember that these American companies are not the enemy. They employ thousands of Americans and provide essential cyberservices to millions of people. They are profit-making entities that want to satisfy their customers and grow their businesses. These American companies have absolutely no motivation to send private customer information to the government or anyone else. In fact, they have every reason to protect it.

Under this legislation, American companies will enhance their capability to protect the private information of their customers by receiving classified assistance from the government. Moreover, they will help their customers and the country by voluntarily informing the government of malware and other malicious conduct and threats that emerge from their networks. But that is not the only way that this bill protects our citizens' privacy. It restricts the government's use and retention of any personal information that companies may choose to share. In addition, it directs the intelligence community inspector general to monitor and report any abuse of users' privacy.

Finally, we must also remember that the government is not the enemy. The intelligence community does not want to squander this opportunity to improve our Nation's cybersecurity by abusing the civil liberties or privacy of American citizens. To this end, the bill specifies that the government can only use the information it receives from the private sector for purposes directly related to addressing cyberthreats, national security, and threats to life and limb.

In closing, this legislation strikes the appropriate balance between the interests of the private sector industry, the Federal Government, and private citizens.

The Acting CHAIR. The time of the gentleman has expired.

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

Mr. BOREN. It will help our country avoid a potential cybercatastrophe that could threaten our national security and endanger our economic prosperity.

With that, I urge my fellow Members to join me and support this important bill.

Again, I want to say specifically to our ranking member and our chairman, thank you for putting the country's interests ahead of partisan gain. We're working together in this committee, both Democrats and Republicans, to do what is in the best interest of our intelligence community and the United States of America.

Mr. RUPPERSBERGER. Madam Chair, may I ask how much time we have on both sides?

The Acting CHAIR. The gentleman from Maryland has 8 minutes remaining, and the gentleman from Michigan has 10½ minutes remaining.

Mr. ROGERS of Michigan. Madam Chair, I yield 1½ minutes to the gentleman from Texas (Mr. BARTON).

Mr. BARTON of Texas. I thank the chairman.

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

My friends, that is the Fourth Amendment to the Constitution, one of the original 10 in the Bill of Rights protecting, in writing, the privacy of the United States citizenry.

I want to give Mr. ROGERS and Mr. RUPPERSBERGER an ''A'' for effort in terms of identifying the problem, but I have to give them an ''F'' for problem solution.

The word ''privacy'' in the underlying bill is mentioned one time, and that in passing. There are no explicit protections for privacy. In fact, there is an explicit exemption of liability to all people who engage in the collection, dissemination, transfer, and sharing of information. The cause of action, if you feel your privacy has been violated, is to go to district court and prove there was willful and knowing sharing of your information without your permission. If you prevail in Federal district court, you get $1,000, or whatever it costs you.

My friends, we have a real problem. I take the chairman at his word—he's a former FBI agent—that he wants to solve this cyberthreat. I know he means it. But until we protect the privacy rights of our citizens, the solution is worse than the problem that they're trying to solve.

Please vote ''no'' on this bill.

Mr. RUPPERSBERGER. Madam Chair, I have no more speakers, and I yield myself such time as I may consume.

First thing, there were some comments that I would like to respond to.

First thing, this bill does not allow the wholesale violation of privacy rights. This bill is extremely important to our national security, but also important to our citizens of this great country, our privacy rights, and civil liberties.

The chairman and I have taken this very seriously, as have the members of our caucus. We know this is not a perfect bill—there will probably be additional changes. We will have more debate later on this afternoon.

Now, some of the things I want to address. During the drafting of this legislation we put forward a wide range of privacy protections. We worked for the last year with the White House, privacy groups, and business groups to come to a coalition to make sure that we get this bill right.

First, the bill severely limits what kind of information can be shared with the government. Only information directly pertaining to the threat can be shared, which is mostly formulas, X's and O's of the virus code. It's almost something that the companies deal with now in dealing with spam.

Second, the bill encourages companies to voluntarily strip out personal information that may be associated with these zeroes and ones. Occasionally, that does occur, and we have to deal with that, and we'll continue to deal with that issue.

There also are strong use limitations on the data. This information must be used for cybersecurity purposes or the protection of national security. The information cannot be used for regulatory purposes. For example, if there's evidence of tax evasion, that information cannot be used in a criminal proceeding, only in national security, only in the areas of life and limb, or for anything involving juvenile crimes.

The bill prohibits the government from requiring the companies to give information to the government in exchange for receiving the cyberthreat intelligence. That means that when we pass the information of the attacks—it's called the secret sauce—to the providers, it's only voluntarily. The government can't put any restrictions on that whatsoever. That really means that this is not surveillance at all.

The bill does not allow the government to order you to turn over private email or other personal information. This is not, again, surveillance.

The bill does not allow the government to monitor private networks, read private emails, censor or shut down any Web site. This is not SOPA.

In an effort to improve the bill even more, the intelligence community—thank you to the leadership of Chairman ROGERS—has been working with privacy groups, the White House, and other interested parties to address these concerns with the legislation. We on our side of the aisle take, again, this issue of privacy very seriously. The committee has maintained an open door policy and made more changes to the bill to make it even better as we have gone on up until today.

The legislation grants no new authority to the Department of Defense, National Security, or the intelligence community that require it to direct any public or private cybersecurity effort. If the government violates any of these restrictions placed on it by the legislation, the government can be sued for damages, costs, and attorneys fees.

I think it is extremely important—we on the Intelligence Committee deal with these issues every day. This is a very sophisticated area that we deal with that most people don't know. So we're attempting, and we have for the last year, to educate as many of our Members as we can. But it's important to know that national security is clear—our effort and what we're attempting to do—but also to maintain the privacy, the constitutional rights of our citizens.

I reserve the balance of my time.

□ 1520

Mr. ROGERS of Michigan. Madam Chair, I yield 2 minutes to the distinguished gentleman from Texas (Mr. THORNBERRY).

Mr. THORNBERRY. Madam Chair, I don't think we can say often enough how important it is that the chairman and ranking member have worked together, not only on the substance of this bill, but in the process of getting us here. They have, truly, put the country's interests first, and I think all Members should commend them for that.

This was a good bill when it was reported out of committee 17–1. I think it will be a better bill once the amendments are considered and adopted. And for any Member who has concerns about privacy or misuse of information, I think they should look at the amendments that are going to be adopted; and any reasonable concern, any semi-reasonable concern about privacy will be addressed with the limitations that those amendments add.

Madam Chair, this bill does not solve all the problems in cybersecurity. All four bills that we're considering today and tomorrow don't solve all the problems we have in cybersecurity. But it makes no sense to me, as some seem to have argued, that we should not solve this problem of information-sharing because we're not solving all the problems that somebody can see out there.

This problem of information-sharing has been central to cybersecurity concerns for some time. I happened across a report from December 2004 that was issued by a subcommittee I chaired of the Select Committee on Homeland Security, along with the gentlelady from California (Ms. ZOE LOFGREN), where we wrote: Whether it is vulnerability assessments, threat warnings, best practices or emergency response, information-sharing with the private sector is critical to securing the United States from cyberattack. That was 8 years ago.

Why has it not occurred? Because all the legal obstacles, all the fear of being sued has prevented it from occurring. And that's what this bill does. It clears away the legal underbrush that has prevented the kind of information-sharing that people have been talking about for a decade.

This is a good, important step. It doesn't solve all the problems, but it puts more information at the disposal of critical infrastructure so that they can be protected. It should be adopted.

Mr. RUPPERSBERGER. Madam Chair, I have a speaker on the way.

Mr. ROGERS, do you have any more speakers?

Mr. ROGERS of Michigan. I do.

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

Mr. ROGERS of Michigan. Madam Chair, I yield 2 minutes to the distinguished gentleman from the great State of Oregon (Mr. WALDEN).

Mr. WALDEN. I thank the chairman and the ranking member for their bipartisan and thoughtful approach to this incredibly important issue facing our country. I support your legislation. I commend you both for identifying a glaring hole in our cyberdefenses: better information-sharing between the private sector and the government.

Such sharing is a force multiplier. It combines the technological strength of our network providers with the ongoing efforts of our agencies to combat growing cyberthreats. From the get-go, the bill has protected privacy and civil liberties and ensured that any information-sharing is voluntary.

I understand Chairman ROGERS has also gone the extra mile to reach out to the privacy community and will be offering and supporting amendments to address any lingering concerns that may remain from misunderstandings over the language. Breaking down the barriers to information-sharing is a linchpin to better cybersecurity, and this legislation will be a tremendous step forward in securing cyberspace for our citizens.

But don't take my word for it. That's what cybersecurity firms and researchers, Internet service providers, and government officials told the Subcommittee on Communications and Technology, which I chair, in the three separate hearings that we held. That's what a bipartisan working group I convened concluded when it interviewed a broad spectrum of stakeholders in the cybersecurity debate.

By contrast, no matter how well-intentioned, cybersecurity regulations would likely just expand government, reduce flexibility, impose costs, misallocate capital, create more red tape and not more security. According to one government witness, regulating cybersecurity practices would ''stifle

innovation and harm the industry's ability to protect consumers from cyberthreats.''

Indeed, voluntary efforts, not government regulation, are already improving cybersecurity for communications networks that cover 80 percent of Americans.

When Congress is looking at a complex issue like cybersecurity, we need to heed the Hippocratic Oath: First, do no harm.

So I want to thank my colleagues for making this process especially open and transparent. Representative ROGERS has graciously reached out to members of the Energy and Commerce Committee to understand our concerns about protecting privacy and civil liberties and preventing regulatory overreach, and Representative THORNBERRY's work in organizing the House Republican Cybersecurity Task Force, which included Representatives TERRY and LATTA, members of my subcommittee.

The Acting CHAIR. The time of the gentleman has expired.

Mr. ROGERS of Michigan. I yield the gentleman an additional 30 seconds.

Mr. WALDEN. The bottom line is, we're going to protect America from the greatest threat to America and to Americans with this legislation. We need to make sure that our private sector is nimble and flexible and innovative; and tying its hands with prescriptive regulation—we heard over and over again in our subcommittee hearings—would do the opposite of that and would result in the bad guys getting an edge on the good guys.

I support this bipartisan legislation. I urge its passage.

Mr. RUPPERSBERGER. Madam Chair, I yield 2 minutes to my distinguished colleague from the State of Georgia, Mr. JOHN LEWIS, one of the most respected Members of our Congress.

Mr. LEWIS of Georgia. Madam Chair, I want to thank my friend, the gentleman from Maryland (Mr. RUPPERSBERGER) for yielding.

Madam Chair, I rise to oppose H.R. 3523. It is a step back.

Those of us who protested in the fifties and the sixties, who were called Communists, who had our telephone calls recorded, we have a long memory. We remember our Nation's dark past.

Martin Luther King, Jr.'s telephone was wiretapped. His hotel room was wiretapped. His home was wiretapped. Our office was wiretapped. Our meetings were wiretapped. And it was not just people spying on civil rights activists, but people protesting against the war in Vietnam.

We didn't have a Facebook, a Twitter, or email. These new tools must be protected. Today we have a mission, a mandate, and a moral obligation to protect future generations of activists and protestors.

So I say to my colleagues, stand with us today. Stand up and stand on the right side of history. Oppose H.R. 3523.

Mr. ROGERS of Michigan. Madam Chair, I yield myself 2 minutes.

Lots of misinformation about this bill today. I respect the gentleman from Georgia greatly for his efforts. I heard the gentleman from Texas talk about searches and seizures. And this is the good news: there are none of those things in this bill. None.

You know, if I knew that your house was to be robbed, I would expect that if the police knew, that they'd pick up the phone and call you and say, you are going to be robbed. Take precaution. We'll be their shortly.

This bill just says, if we have this nasty source code, these zeroes and ones, I want to give it to you so you can protect your systems. That's it. No monitoring, no content, no surveillance, nothing. That's not what this bill is about.

I understand the passion about it. That's why we've taken a year to forge this bipartisan effort to get where we believe privacy is protected. It is paramount that we do that, that our civil liberties are protected. It is paramount that we do that.

But we at least take down the hurdle to share nasty source code or software that's flying through the Internet, that's developed, and it's very sophisticated, by the Chinese and the Russians and the Iranians and other groups and non-nation-state actors that are going to steal your personal information.

That's all this is. It's sharing bad source code so you can put it on your system so you don't get infected. End of story.

I wish people would read the bill, all of it, every word of it. I think you'll find the carefully crafted language to make sure that our rights are protected, that the Fourth Amendment is protected.

And by the way, just like the Army, the Navy, the Marines, your FBI is protecting you. That's what this bill allows it to do, simply that.

So, as I said, I respect greatly the gentleman from Georgia. There's a lot of atrocities I think he lived through in his life that no one should have to live through. We took those things into consideration when we wrote this bill, and that's why we've got so much support and so much technical company support, companies like Facebook and Microsoft and all of those groups.

So I hope people read the bill and support the bill.

I reserve the balance of my time.

□ 1530

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

In closing, I want to say again that the purpose of this bill, as the chairman just said, is very basic and simple. We want to protect our citizens from attacks. We are being attacked as we speak right now. Just last year, it was estimated we lost $300 billion worth of trade secrets. We even know that one country is attacking a fertilizer company to find out how we make it better than they do. This is putting our businesses in jeopardy and jobs in jeopardy, and we know we sure need jobs.

More importantly, those of us who work in this field know how serious these threats are. The head of our FBI, whose responsibility it is to provide our domestic national security, has said that one of the most serious threats, if not a bigger threat, in terrorism would be a catastrophic cyberattack. We've already talked today about what that would be. We have Secretary Napolitano, the Director of Homeland Security, who has said the same thing: that it is one of the most serious issues our country has to deal with. It's unfortunate, but most of our citizens aren't aware of how serious this threat is.

So we've attempted to allow our intelligence community, which is one of the best in the world, to have the ability to see these threats coming in from other countries or from terrorist groups and to be able right now to give this information over to the private sector to protect us, you, me, our businesses. That's what this bill does. Nothing more. What we're attempting to do is to move the bill and get the bill to the Senate.

We can always do better in the area of privacy and civil liberties, and we're going to continue to do that. We can always do better in the area of homeland security and go further to protect those institutions and our grid systems and that type of thing; but this is the start, because the one thing that now is stopping our country and is stopping us from protecting our citizens is this Congress.

This Congress needs to pass this bill now. We need to move forward. We need to get it to the Senate. We need to start working with the Senate. Then hopefully we'll deal and work very closely with the White House and find a bill so that we can protect our citizens and also protect our civil liberties and privacy.

I also understand Mr. LEWIS. We all respect him and what he has gone through. As a former prosecutor and lawyer who has worked on many search and seizure warrants and that type of thing, I can tell you this: there are no violations in this bill at all. That is not what this bill is about. If it were, I wouldn't be in favor of it.

I thank you, Mr. ROGERS, for your cooperation and for working with us in this bipartisan manner. It is a very serious issue.

I yield back the balance of my time.

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

I do want to thank the ranking member and both staffs from both committees who have been tireless in this effort to get it right and to find that right place where we could all feel comfortable.

The amendments that are following here are months of negotiation and work with many organizations—privacy groups. We have worked language

with the Center for Democracy and Technology, and they just the other day said they applauded our progress on where we're going with privacy and civil liberties. So we have included a lot of folks.

It has been a long road. It has been the most open and transparent bill that, I think, I've ever worked on here. We kept it open to the very end to make sure that we could find the language that clarified our intent to protect privacy, to protect civil liberties, and to just be able to share dangerous information with victims. That's all this bill is. The whopping 13 pages it is does only that. So I appreciate the comments today. I look forward to the amendment debate.

Again, Mr. RUPPERSBERGER, it has been a joy to work with you on this particular issue.

As an old Army officer once told me, once you find a problem, you are morally obligated to do something about it. We set about it a year ago to make America safe and to protect your network at home from people stealing it, breaking it, and doing something worse.

So, Madam Chair, I look forward to the debate on the amendments, and I yield back the balance of my time.

Mr. CUMMINGS. Madam Chair, although I am voting against the Cyber Intelligence Sharing and Protection Act of 2011 today, I recommend Representative C.A. ''DUTCH'' RUPPERSBERGER, the Ranking Member of the House Intelligence Committee, for his efforts to improve the bill significantly since its passage out of committee. He has been a leader in protecting our Nation against cyber attacks, and he has gone out of his way to make this bill as inclusive and bipartisan as possible. I want to thank him for the time he took to meet with me personally to discuss this legislation and ways to improve it going forward.

I oppose this bill in its current form for several reasons. First, the Republicans on the House Rules Committee refused to allow debate on an amendment offered by Representative BENNIE THOMPSON, the Ranking Member of the House Committee on Homeland Security, to expand this legislation to protect our Nation's critical infrastructure.

In testimony before the House Intelligence Committee, then-CIA Director Leon Panetta called cybersecurity ''the battleground for the future.'' Our Nation's critical infrastructure—including power distribution, water supply, telecommunications, and emergency services—has become increasingly dependent on computerized information systems to manage their operations and to process, maintain, and report essential information. Any effort to address this national security threat must address our Nation's critical infrastructure.

In addition, the legislation includes several provisions that are problematic. For example, under the information-sharing provisions of the bill, private entities receive absolute immunity from criminal or civil liability for any harm that may result from a company's actions that stem from the sharing or receiving of cyber threat information as long as the company can show it was acting in good faith.

This bill would also create a new exemption to the Freedom of Information Act that is unwarranted since current law exemptions provide the flexibility necessary to protect sensitive information. The bill would prohibit agencies from disclosing ''cyber threat information,'' and it would hold the government liable for such disclosure. Unfortunately, an amendment offered on the floor did not sufficiently address these concerns.

Finally, the bill would allow companies to share private consumer data without adequate protections or oversight. Private entities would decide the type and amount of information to share with the Federal Government, and nothing in the bill would require companies to strip out unnecessary personally identifiable information. Again, an amendment offered on the floor did not go far enough to adequately address this issue.

I appreciate the great effort that went into pulling this bill together, but more work is needed before I can offer my support. It is critical that we protect Americans from cyber attacks, and I hope we can continue to improve this legislation as we move forward.

Mr. NADLER. Madam Chair, I rise in strong opposition to H.R. 3523, the Cyber Intelligence Sharing and Protection Act (CISPA).

The main topic this week, as announced by the House Republican Leadership, is cyber security, a serious issue for our Nation. As we become more dependent on computers and technology for even common or routine actions that happen every day, we become at increased risk of great damage from a cyber attack. Nations or individuals who wish us harm know that, and so we must be vigilant.

What we are considering today is premised on the idea that greater information sharing of cyber threats between the government and the private sector will improve security. While this is a relatively uncontroversial idea in concept, the bill before us raises a number of concerns.

It is important to note at the outset that the bill allows companies to share information, including private e-mails and other Internet communications, with the government—notwithstanding any other law. So, protections in existing law, such as the Electronic Communications Privacy Act (ECPA) and the Wiretap Act, are totally superseded. The government could get all of your information without a warrant or subpoena, and you would have little ability, if any, to stop it. Such a blanket exemption should give us great pause.

Unfortunately, the rest of the bill does not provide sufficient safeguards to justify this blanket exemption. To begin with, the definition of the cyber threat information to be shared is very broad. Suggestions have been made that define what should be included as cyber threat information in a narrow but sufficient way. These suggestions were not included in this bill.

At the very least, companies and other entities providing the government with information should be required to take some reasonable steps to remove personally identifiable information. Such reasonable steps need not be overly burdensome, but, again, even this limited protection was not included.

Once this information was shared with the government, it could be reviewed and used by any department. The Department of Defense, National Security Agency, and other defense and intelligence agencies thus would have access to the private, domestic internet activities of innocent Americans. This mixing of domestic information with military entities is dangerous and unprecedented. In fact, our policy has long-been to keep the military out of such domestic affairs. Information about cyber security should be limited to the relevant domestic government bodies, such as the Department of Homeland Security.

The power of government to use the information it receives would also be tremendously broad. One allowable use for this information is the hopelessly vague ''national security.'' In the past, the government has considered peace groups, civil rights activists, and other advocates to be ''threats'' to national security. It is easy to imagine how this term could be utilized for all the wrong reasons. The bill is supposed to be about cyber security, but allowing use of the information collected for national security purposes does not necessarily serve that purpose.

Further, the bill makes enforcing even the limited restrictions it contains difficult. With respect to private entities, as long as they act ''in good faith,'' they are immune from any civil or criminal case in state or federal court. This low standard means that any time a company claims it thought it was following the law, persons harmed by the improper sharing of information will have no recourse.

The bill does allow for civil actions against government violations. Unfortunately, the ability to bring a lawsuit against the government, as provided for in the bill, is deficient in three ways.

First, the bill only would allow lawsuits against the government for breaches if filed ''not later than two years after the date of the violation.'' That time period is wholly unworkable, unfair, and unrealistic.

Second, as written the bill only would impose liability on the government only for ''intentionally'' or ''willfully'' violating its restrictions. While this is helpful, such a limited liability scheme ignores damages arising from negligence. Such negligent acts could involve the failure to properly protect sensitive information or the failure to act with due care in deciding what information should be used.

Lastly, the only remedy is monetary damages. Injunctive relief, which could force the government to change its practices, is not provided for.

I filed an amendment with the Rules Committee to solve these three problems regarding the ability to hold the government accountable. It was not made in order.

In fact, multiple amendments were filed with the Rules Committee which would have made significant improvements to this bill. They would have narrowed its terms, limited how information could be used, protected personal information, and so on. The Rules Committee chose not to make them in order. Some of the amendments the House was allowed to consider will improve the bill, but not enough to sufficiently protect our privacy and civil liberties.

In closing, I want to reiterate that I recognize the importance of the issue of cyber security. I agree with the proponents of the bill that we must improve our cyber security defenses.

But, I remain firmly committed to the notion that we can protect our security and maintain our liberty, privacy, and freedom. This bill puts our privacy at great risk, and unnecessarily so. As such, I oppose its passage and recommend my colleagues do the same.

Mr. RAHALL. Madam Chair, I recognize the need to address the threats posed to our Nation and the American economy in cyber

space, but I also believe we must be very careful in maintaining the appropriate balance between protecting our national security and preserving our civil liberties.

Given the concerns about this measure and the perceived threat to sensitive and personal information of American citizens, I believe that the House should take additional time to deliberate on this measure. The American public deserves an opportunity to gain a fuller understanding of the provisions included in this bill and how their daily lives may be affected by it.

For these reasons, I will oppose the bill.

The Acting 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 112–20. 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:

H.R. 3523

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

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) certified entities; 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 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 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;

''(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) if shared with the Federal Government—

''(i) shall be exempt from disclosure under section 552 of title 5, United States Code;

''(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

''(D) 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.—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—

''(A) for using cybersecurity systems or sharing information in accordance with this section; or

''(B) for decisions made based on cyber threat information identified, obtained, or shared under this section.

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

''(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) for any lawful purpose only if—

''(A) the use of such information is not for a regulatory purpose; and

''(B) at least one significant purpose of the use of such information is—

''(i) a cybersecurity purpose; or

''(ii) the protection of the national security of the United States.

''(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)(B).

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

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

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

''(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)(C) 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)(C) 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)(C) or subsection (c).

''(e) REPORT ON INFORMATION SHARING.—

''(1) REPORT.—The Inspector General of the Intelligence Community 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 review of the sharing of such information within the Federal Government to identify inappropriate stovepiping of shared information; and

''(F) any recommendations of the Inspector General for improvements or modifications to the authorities under this section.

''(2) FORM.—Each report required under paragraph (1) 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

''(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.

''(h) DEFINITIONS.—In this section:

''(1) 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.

''(2) CYBER THREAT INFORMATION.—The term 'cyber threat information' means information directly pertaining to a vulnerability of, or threat to, a system or network of a government or private entity, including information pertaining to the protection of a system or network from—

''(A) efforts to degrade, disrupt, or destroy such system or network; or

''(B) efforts to gain unauthorized access to a system or network, including efforts to gain such unauthorized access to steal or misappropriate private or government information.

''(3) CYBER THREAT INTELLIGENCE.—The term 'cyber threat intelligence' means information in the possession of an element of the intelligence community directly pertaining to a vulnerability of, or threat to, a system or network of a government or private entity, including information pertaining to the protection of a system or network from—

''(A) efforts to degrade, disrupt, or destroy such system or network; or

''(B) efforts to gain unauthorized access to a system or network, including efforts to gain such unauthorized access to steal or misappropriate private or government information.

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

''(5) CYBERSECURITY PURPOSE.—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—

''(A) efforts to degrade, disrupt, or destroy such system or network; or

''(B) efforts to gain unauthorized access to a system or network, including efforts to gain such unauthorized access to steal or misappropriate private or government information.

''(6) CYBERSECURITY SYSTEM.—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—

''(A) efforts to degrade, disrupt, or destroy such system or network; or

''(B) efforts to gain unauthorized access to a system or network, including efforts to gain such unauthorized access to steal or misappropriate private or government information.

''(7) 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.

''(8) 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.

''(9) 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)(3) 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)(9) of such Act, as added by subsection (a)).

(c) INITIAL REPORT.—The first report required to be submitted under 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 one year after the date of the enactment of this Act.

(d) 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.''.

The Acting CHAIR. No amendment to that amendment in the nature of a substitute shall be in order except those printed in House Report 112–454. 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. LANGEVIN

The Acting CHAIR. It is now in order to consider amendment No. 1 printed in House Report 112–454.

Mr. LANGEVIN. I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 1, line 13, strike ''UTILITIES'' and insert ''CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS''.

Page 2, line 1, strike ''utilities'' and insert ''critical infrastructure owners and operators''.

Page 3, line 13, strike ''utility'' and insert ''critical infrastructure owner or operator''.

Page 3, line 16, strike ''utility'' each place it appears and insert ''critical infrastructure owner or operator''.

Page 17, strike lines 12 through 16.

The Acting CHAIR. Pursuant to House Resolution 631, 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.

The bill that we are considering today creates a voluntary information-sharing network, which could provide owners and operators of critical infrastructure with valuable threat information that would help them to secure their networks from cyberattacks.

Unfortunately, the legislation specifies that it applies only to ''private sector entities and utilities.'' While ''utilities'' is defined extremely broadly in the legislation as any entity that provides ''essential services,'' including telecommunications and transportation providers, there remains the possibility that the definition may exclude pieces of our critical infrastructure that have significant cybervulnerabilities.

My amendment, which I am offering with my good friend Mr. LUNGREN from California, strikes the uses of the word ''utilities'' and replaces it in each instance with the phrase ''critical infrastructure owners and operators.'' This is a commonsense way to avoid potential confusion and to eliminate any possibility that critical entities could be denied the opportunity to opt into this voluntary information-sharing framework and thereby share and receive the valuable classified threat information that will be available under CISPA.

This amendment will not significantly expand the scope of the legislation, but instead will help prevent interpretations of language that could be contrary to the committee's intent, which I believe is the same as mine.

Now, while I recognize that any regulation of critical infrastructure would be outside the Intelligence Committee's jurisdiction, I nonetheless want to take this opportunity to voice my strong conviction that our efforts must not stop with the legislation that we are considering this week.

Just as the airline industry must follow Federal Aviation Administration safety standards, the companies that own and operate the infrastructure on which the public most relies should be accountable for protecting their consumers when confronted with a significant risk. I, along with many Members on both sides of the aisle and experts within and outside of government, have come to the same basic conclusion: the status quo of voluntary action will not result in strong cyberprotections for our most valuable and vulnerable industries. The Secretary of Homeland Security emphasized last week that our critical infrastructure control systems, which are mainly in private hands, must come up to a certain baseline level in cybersecurity standards.

With increased public awareness helping to build momentum for legislative action, we have a real chance to address these threats. I hope that we will not look back on this moment years from now, regretting a missed opportunity after the damage has been done. While the amendment we are offering today will not by itself provide the protections that Mr. LUNGREN and I ultimately believe are necessary for our critical infrastructure, it is a useful first step, and I am thankful to Mr. LUNGREN for joining me in this effort.

With that, Madam Chair, I reserve the balance of my time.

Mr. ROGERS of Michigan. I rise in opposition to the amendment.

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

Mr. ROGERS of Michigan. I want to first compliment Mr. LANGEVIN for working with us on the cybersecurity bill. He has been an instrumental force in pushing this cybersecurity issue to the front and in getting the language that we have that finds that right balance.

My concern with this, which is why I thought, at least, the President's advisers who were recommending to him that he veto the bill were misguided, is that now we have done something in this bill that is fairly unique. It is all voluntary, and we have separated the government and the private sector. The government is not going to be involved in private sector networks, and they're not going to be involved in the government networks. Perfect. That's exactly the balance we found.

With this, it crosses both of those, and it gets us to a place that I think we need to have a lot more discussion on, and you can see by the level of debate just on this issue how people are really nervous about the Federal Government getting into their business.

□ 1540

This, I'm afraid, opens it up to that. Here's the good news. We believe this is already covered in the bill as far as the sharing component, and you replace the word ''utility'' with something that isn't defined, ''critical infrastructure, owners and operators.'' We're not sure what that is, and in some cases you could extrapolate that to be even the local police, who argue they're part of the national security infrastructure. Does that mean local police are going to get very sensitive foreign cyberintelligence information? And why would they have it? We don't know the answers to those questions, and that's why we're having such a hard time with this amendment.

I would argue that there does need to be a Homeland Security bill, and it really shouldn't be done in the Intelligence Committee. It should be done in the Homeland Security Committee.

So I would love to work with Mr. LANGEVIN as the process works its way through the Homeland Security Committee and believe that that should be fully debated.

Remember, when you start getting regulation into the private sector, including private networks, that, I argue, is troublesome and very worrisome to me, and something I would have a hard time supporting.

So, I look forward to working with the gentleman. I would have to oppose this amendment, but I want to thank you for all your work on the cyberissue and, clearly, this cyber information-sharing bill.

I reserve the balance of my time.

Mr. LANGEVIN. I thank the chairman of the Intelligence Committee for his thoughts. I respectfully disagree. The word ''utilities'' is important, but I believe ''critical infrastructure,'' out of an abundance of caution, is a better term than ''utilities''.

How much time do I have, Madam Chair?

The Acting CHAIR. The gentleman has 2 minutes remaining.

Mr. LANGEVIN. I yield 1½ minutes to the distinguished chairman on the Department of Homeland Security Committee, the gentleman from California (Mr. DANIEL E. LUNGREN).

Mr. DANIEL E. LUNGREN of California. I think the amendment is quite simple. As written, the bill allows for information to be shared with the private sector and utilities, but there are those that do not fall within that that I think we would all agree should be able to have this relationship.

Our amendment would have the simple effect of including those elements such as airport authorities, mass transit authorities, or municipal hospitals, which are neither private sector nor utilities, to be able to participate in this voluntary information-sharing regime.

I find it odd to find out that the committee is worried about the definition of ''critical infrastructure.'' That has been defined in the U.S. Code for over a decade. It is in the language in 42 U.S.C. 5195c, the Critical Infrastructure Protection Act of 2001, which defines critical infrastructure as:

> Systems or assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

That has been the definition that we have supported. That's been the definition that we've worked on. Your committee, our committee, all committees have. I find this a very simple amendment that tries to reach what we are all trying to reach. It does not grant any more authority to the Federal Government. It allows for the sharing of information to vital entities, as the gentleman has suggested, that we would all agree ought to be there.

I would hope that pride of authorship is not the problem here. We're trying to do something that we think makes common sense. And if folks have trouble with the definition of critical infrastructure, you would have thought it would have been raised in the last decade.

The Acting CHAIR. The time of the gentleman has expired.

Mr. LANGEVIN. I yield the gentleman an additional 15 seconds.

Mr. DANIEL E. LUNGREN of California. I would hope that we could have support for this bipartisan amendment brought forward by the gentleman who

serves on the Intelligence Committee. I serve on the Homeland Security Committee. I'm chairman of the Subcommittee on Cybersecurity.

It seems to me to make imminent sense. I do not understand why there is some opposition to this amendment. I thank the gentleman.

Mr. ROGERS of Michigan. How much time do I have remaining?

The Acting CHAIR. The gentleman has 3 minutes remaining.

Mr. ROGERS of Michigan. I would just remind the gentleman that the definition does not go back anywhere in this bill to that. It leaves it open, and when you start, again, crossing that valley between the government and the private sector, it causes serious issues—as you can see, the people who are very concerned that the government is going to get into regulating anything on the Internet.

I would say this is no pride of authorship. I don't know if Mr. RUPPERSBERGER and I could have any more authors participate in our bill than we have.

The problem here is very real and very substantive. And that's why I think both the gentlemen, who have as much passion and care and commitment to this issue as I've seen, need to work that issue on the Homeland Security Committee so you can do it in a way that won't rise to the level of the objections that we have seen when just the suggestion of regulating outside of the purview of national security comes into discussion.

That's why I would hope the gentleman would exercise extreme caution when taking that walk. It is perilous for the government to get into regulating the Internet, and I oppose that completely. That's why we have these problems, I think, arise from it. I think, if these are issues that they can get over, that this should have substantive debate. Remember, this very narrow bill took 1 year—1 year—of work and negotiation and discussions to get it to where we are today.

So, I would encourage that maybe more thought ought to be put in it, and I would look forward to working with both gentleman as they introduce and work their bills through the Homeland Security Committee, as I think would be appropriate.

I reserve the balance of my time.

Mr. LANGEVIN. Again, I thank the chairman of the Intelligence Committee for his thoughts. I want to be very clear that this term substituting ''critical infrastructure'' for ''utilities'' does not lend to regulating critical infrastructure. It just allows for the broadest possible definition of information-sharing among those entities that are deemed to be critical infrastructure.

With that, I thank Chairman LUNGREN for his support of this bipartisan amendment, and I yield back the balance of my time.

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

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

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

Mr. LANGEVIN. Madam Chair, I demand a recorded vote.

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

The Chair understands that amendment No. 2 will not be offered.

AMENDMENT NO. 3 OFFERED BY MR. POMPEO

The Acting CHAIR. It is now in order to consider amendment No. 3 printed in House Report 112–454.

Mr. POMPEO. I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 8, beginning on line 18, strike ''or sharing information'' and insert ''to identify or obtain cyber threat information or for sharing such information''.

The Acting CHAIR. Pursuant to House Resolution 631, the gentleman from Kansas (Mr. POMPEO) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Kansas.

Mr. POMPEO. I want to thank Chairman ROGERS and Chairman RUPPERSBERGER for their hard work on this important piece of legislation. I am among those folks who, when I first learned of this legislation, had some concerns to make sure that it was balanced and it did the right things. Also as a former Army officer, I recognize the deep national security implications of the cyberthreat, but I also wanted to make sure that we also did everything that was necessary to protect everyone's privacy rights.

This is a simple amendment. It makes clear that the liability protection in the bill with respect to the use of such systems only extends to the identification and acquisition of cyberthreat information and no further.

This is an unprecedented threat from countries like China and Russia. These are hostile nations, and they're committing resources, unprecedented resources, to attack U.S. networks each and every minute of every day. While this new threat is being developed by our foreign enemies, organized criminals and foreign hackers also just as easily deploy malicious cyberattacks to disrupt stock markets, transportation networks, businesses, governments, and even our military operations.

A devastating cyberattack could easily be unleashed from the remote comfort of enemies' computers thousands of miles away from our Nation. We must take this threat very, very seriously.

Part of the challenge in cyberspace is that a line of computer code could be just as deadly as a traditional military weapon. We've already seen these attacks used as an instrument of war. In 2008, Georgia suffered a significant cyberattack prior to the invasion by Russia. This attack crippled Georgia's banking system and disrupted the nation's cell phone services, helping to clear the battlefield for the invading Russians.

Perhaps the most significant dangerous activity in cyberspace even goes unnoticed. Cyberspies lay in wait for years in order to eventually steal precious military and economic secrets. Each of these examples further illustrates the need for legislation. Unfortunately, some civil liberties and privacy advocates claim that liability protection in this bill with respect to the use of cybersecurity systems could lead to broader activities than authorized.

This legislation doesn't do that, but my amendment simply provides clarifying language to the original language of the bill, and thus enjoys the support of bipartisan cosponsors of the legislation, as well as the outside groups that raise these concerns.

Madam Chair, I urge approval of this amendment.

With that, I reserve the balance of my time.

The Acting CHAIR. Does any Member seek time in opposition?

Mr. POMPEO. I yield as much time as he may consume to the gentleman from Michigan (Mr. ROGERS), the chairman of the Intelligence Committee.

□ 1550

Mr. ROGERS of Michigan. I want to thank Mr. POMPEO for working with us. This was an amendment negotiated with Mr. RUPPERSBERGER and myself and Mr. POMPEO to clearly define the intention of the bill, and I think it offers protections. I think we should all strongly support Mr. POMPEO's amendment.

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

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

The amendment was agreed to.

AMENDMENT NO. 4 OFFERED BY MR. ROGERS OF MICHIGAN

The Acting CHAIR. It is now in order to consider amendment No. 4 printed in House Report 112–454.

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

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 9, beginning on line 2, strike ''affect any'' and insert ''affect—''.

Page 9, strike lines 3 through 5 and insert the following:

''(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.

The Acting CHAIR. Pursuant to House Resolution 631, 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. Madam Chair, I strongly encourage the support of this amendment. It's a simple amendment we negotiated. It is clarifying language again on FOIA.

With that, I yield such time as he may consume to the gentleman from California (Mr. ISSA).

Mr. ISSA. I thank the gentleman for yielding. Hopefully there will be time left over also for Mr. CHAFFETZ, who has worked hard on this amendment.

I want to thank the chairman for working with our committee on this amendment that clarifies in the Cyber Intelligence Sharing and Protection Act that FOIA, the Freedom of Information Access Act, is in fact clearly in effect for the vast majority of this information.

We understand that companies—I will just take an example—such as electric utility companies may share their very vulnerabilities as a part of a process to reduce or eliminate these vulnerabilities. We certainly understand that that's not FOIAable. National security is not FOIAable. However, we, in this amendment, ensure that everything is at least possibly FOIAable whenever it would be appropriate, and then the only question is does it stand for one of the exclusions. So by making it narrow, we tell the American people that the Freedom of Information Act is in effect on cybersecurity and will not be unreasonably withheld.

I think this is critical at a time when greater transparency is the promise and there is a great deal of concern about cybersecurity somehow being something that would take away America's freedoms. Just the opposite is true. Our freedom of the Internet, our freedom to have an effective and efficient system on which to build our infrastructure both for electricity and other utilities, but also for our everyday life, essentially requires the kind of cooperation that we anticipate.

Mr. RUPPERSBERGER. Madam Chair, I claim time in opposition to the amendment; however, I do not oppose the amendment.

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

There was no objection.

Mr. RUPPERSBERGER. I agree with Mr. ISSA's comments. This is a joint amendment of Mr. ROGERS and me. The amendment would make it clear that while FOIA exemption protects information obtained under the bill, regulatory information required by other authorities remains subject to FOIA requests.

The chairman and I agree the law should not create a broad change. The type of information that is available under the Freedom of Information Act, we have a responsibility to protect classified information from disclosure, but we also understand the need to keep information open to the public. The amendment makes clear that information available under other authorities remains subject to FOIA, and I urge all Members to support this bipartisan amendment.

Mr. CHAFFETZ. Will the gentleman yield?

Mr. RUPPERSBERGER. I yield to the gentleman from Utah.

Mr. CHAFFETZ. I thank the gentleman for yielding.

I appreciate the bipartisan nature in which this is moving forward. I appreciate specifically Chairman ROGERS, Chairman ISSA, and the ranking member.

I stand in support of this amendment. I think FOIA is a very important principle we have in this, and this just strengthens that.

I would also say, Madam Chair, that I was opposed to SOPA. I was adamantly opposed to this. But this bill in particular is desperately needed in this country. Cybersecurity is a very real threat, and this bill is something that is needed in this country. I think it is strong in its Fourth Amendment protections. I think it's appropriate for this Nation to do this. We need to make sure that we're smart in how we advance.

There have been some much-needed amendments that were adopted. But again, the bill, as we see it moving forward, I think, will strengthen cybersecurity in this country, and I'm proud of the fact that Chairman ROGERS is bringing this bill to the floor.

I urge the support of this amendment and the underlying bill.

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

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

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

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

Mr. RUPPERSBERGER. Madam Chair, I demand a recorded vote.

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

It is now in order to consider amendment No. 5 printed in House Report 112–454.

AMENDMENT NO. 6 OFFERED BY MR. QUAYLE

The Acting CHAIR. It is now in order to consider amendment No. 6 printed in House Report 112–454.

Mr. QUAYLE. Madam Chair, I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 9, strike lines 8 through 18 and insert the following:

''(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;

''(D) for the protection of minors from child pornography, any risk of sexual exploitation, and serious threats to the physical safety of such minor, 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 2258A(a)(2) of title 18, United States Code; or

''(E) to protect the national security of the United States.

Page 16, before line 1 insert the following:

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

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

''(i) efforts to 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).''.

The Acting CHAIR. Pursuant to House Resolution 631, the gentleman from Arizona (Mr. QUAYLE) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Arizona.

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

I appreciate the opportunity to speak in favor of this bipartisan amendment that I'm offering along with Congresswoman ESHOO, Congressman THOMPSON, and Congressman BROUN.

H.R. 3523 is designed to increase the sharing of government intelligence and cyberthreats with the private sector and allow private sector companies to share threat information on a voluntary basis. The bill is consistent with our founding principles and our Constitution. Indeed, as the nature of the threats facing our Nation change, I believe this legislation is vital to protecting our country.

Every day our military intelligence communities work to counter traditional threats like nuclear and biological weapons in order to prevent a catastrophic attack on U.S. soil, but today's security threats are becoming less traditional. Four nations have chosen cyberspace as an area of particular

vulnerability for America and are targeting critical military and economic cyberinfrastructure.

Admiral Mike Mullen, the former Chairman of the Joint Chiefs of Staff, lists cyberattacks as one of the top threats facing the United States. Secretary of Defense and former CIA Director Leon Panetta warned that the next Pearl Harbor we confront could very well be a cyberattack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems.

This legislation not only protects our national security and intellectual property, it also provides private and public entities to voluntarily work with the government to protect every individual's personal information from nation-state actors like China, Russia, and Iran, who are determined to use cyberattacks to steal from us and weaken us.

□ 1600

This bipartisan amendment will further solidify protecting the homeland from foreign nation-states wishing to do us harm, while protecting civil liberties.

This amendment significantly narrows the bill's current limitation of the Federal Government's use of cyberthreat information that is voluntarily shared by the private sector. Specifically, this amendment strictly limits the Federal Government's use of voluntarily shared cyberthreat information to the following five purposes: cybersecurity purposes; investigation and prosecution of cybersecurity crimes; protection of individuals from danger of death or serious bodily harm; and protection of minors from child pornography, any risk of sexual exploitation, and serious threats to the physical safety of a minor; finally, protection of the national security of the United States.

If the government violates the use limitation, the bill provides for government liability for actual damages, costs, and attorney fees in Federal court. These provisions together ensure that information cannot be shared with the government or used under this bill unless there's a direct tie to cybersecurity.

Cyberterrorists work fast, so Congress needs to work faster to protect America. Enabling information-sharing between the government and private sector is the quickest and easiest way to prevent a cyberattack on our Nation. Our amendment ensures we can accomplish this goal while also protecting the privacy of all Americans, and I urge my colleagues to support it.

Mr. RUPPERSBERGER. I rise to claim time in opposition, but I do not oppose the amendment.

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

There was no objection.

Mr. RUPPERSBERGER. I yield to the gentleman from California (Mr. THOMPSON). He is on the Intelligence Committee and also a sponsor of this amendment.

Mr. THOMPSON of California. I thank the gentleman for yielding.

Madam Chair, I rise in support of the Thompson-Eshoo-Quayle-Broun amendment to this bill. The threat of a devastating cyberattack is real and cannot be understated. I believe the Federal Government and private companies need to work together to protect our national and economic security. But in doing so, we still have a responsibility to protect the constitutional rights of law-abiding citizens.

I'm concerned that the underlying bill is drafted in a way where consumer information could be shared too broadly and used in ways unrelated to combating cybersecurity threats. The Thompson-Eshoo-Quayle-Broun amendment will tighten the bill's limitation on the Federal Government's use of cyberthreat information shared under this legislation. Specifically, our amendment will limit the Federal Government's use of shared information only for cybersecurity purposes, for the investigation and prosecution of cybersecurity crimes, to protect against the threat of imminent harm, and protect our country's national security.

This bill, even with our amendment, isn't perfect. As this legislation moves forward, I expect the word of the chairman to be honored when he says that our committee will work together to further protect personal information and limit its use. For example, further narrowing terms in this bill, such as ''to protect the national security of the United States,'' will be necessary, I believe, to fully protect our civil liberties.

Mr. QUAYLE. I yield 30 seconds to the chairman of the Intelligence Committee, Mr. ROGERS.

Mr. ROGERS of Michigan. Thank you, Mr. QUAYLE.

Again, this is an amendment worked out with Mr. RUPPERSBERGER, Mr. THOMPSON, Mr. QUAYLE, and myself. Ms. ESHOO is also on the amendment.

This is in consultation with all of the privacy groups and the civil liberty groups. We wanted to make sure that the intent matched the language. And we think this is a limiting amendment on what it can be used for, which is very narrow, is very specific; and we think this enhances already good privacy protections in the bill, and I strongly support it and would encourage the House to strongly support the bipartisan amendment.

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

Mr. QUAYLE. I just want to thank the chairman and the ranking member and their staffs for working tirelessly on this bill. It's a good bill, and this amendment, I believe, strengthens it.

I urge my colleagues to support it, and I yield back the balance of my time.

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

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

Mr. RUPPERSBERGER. Madam Chair, I demand a recorded vote.

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

AMENDMENT NO. 7 OFFERED BY MR. AMASH

The Acting CHAIR. It is now in order to consider amendment No. 7 printed in House Report 112–454.

Mr. AMASH. I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 10, after line 10, insert the following new paragraph:

''(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):

''(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.

The Acting CHAIR. Pursuant to House Resolution 631, the gentleman from Michigan (Mr. AMASH) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Michigan.

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

I'm extremely concerned about the privacy implications of the bill. The liability waiver goes too far, and the government can access too much of Americans' private information and use it in too many ways.

Our amendment addresses that last concern. Our amendment prohibits CISPA from being used to snoop through sensitive documents that can personally identify Americans. The documents that our amendment makes off-limits to the government are library and book records, information on gun sales, tax returns, educational records, and medical records.

We didn't pull this list out of thin air. In fact, the list already exists in Federal law as part of the PATRIOT Act. Under the PATRIOT Act, the Federal Government can obtain these documents as part of a foreign intelligence investigation only if senior FBI officials request the documents and a Federal judge approves.

Many have questioned the wisdom of allowing the government access to sensitive documents even in those more limited circumstances. If the PATRIOT Act requires the approval of a Federal judge and a senior FBI official, surely we can't allow access to such personal information without any judicial or agency oversight. I don't know why the

government would want to snoop through library lists or tax returns to counter a cyberattack. But if the government wants these records, it has existing legal processes to obtain them. Our constituents' privacy demands that we not give the government unfettered and unsupervised access to these documents in the name of cybersecurity.

Please support the bipartisan Amash-Labrador-Nadler-Paul-Polis amendment.

I reserve the balance of my time.

The Acting CHAIR. Does any Member seek recognition in opposition to the amendment?

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

Mr. NADLER. Madam Chair, I rise in strong support of the Amash-Labrador-Nadler-Paul-Polis Amendment.

While I believe most Members agree both that a cyber attack could be devastating and that sharing information will help to fight that threat, the underlying bill is overly broad and intrusive. Our amendment will add at least a modicum of protection for Americans' privacy.

While the idea of privacy may seem quaint to some in this day of social networking and the Internet, most Americans still believe that they have a zone of privacy vis-a-vis the government. As such, it is important we protect private actions from the prying eyes of government. Moreover, the government has a history of misusing such information and so we need to be very circumspect in what we allow it access to.

Our amendment prohibits records or information regarding what books you bought or checked out of the library, your medical records, tax returns, and so on from being used by the government for any purpose if it obtained that information pursuant to this bill. There is no need for the government to have this most personal of information—I don't see how any of it could be possibly relevant to cyber security. And, if the information can't be legally used, hopefully that will discourage companies from sharing it in the first place.

The categories of information in our amendment are already given a protected status in the Foreign Intelligence Surveillance Act (FISA). FISA requires a court order and the approval of a high-ranking FBI official to request these personal materials. If that is the standard under FISA, we should not let companies cavalierly hand such records to the government with no independent review at all.

I urge my colleagues to support this amendment.

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

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

Mr. AMASH. Madam Chair, I demand a recorded vote.

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

AMENDMENT NO. 8 OFFERED BY MR. MULVANEY

The Acting CHAIR. It is now in order to consider amendment No. 8 printed in House Report 112–454.

Mr. MULVANEY. I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 10, after line 10 insert the following:

''(4) 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).

''(5) 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).

''(6) PROTECTION OF INDIVIDUAL INFORMATION.—The Federal Government may, consistent with the need to protect Federal systems and critical information infrastructure from cybersecurity threats and to mitigate such threats, undertake reasonable efforts to limit the impact on privacy and civil liberties of the sharing of cyber threat information with the Federal Government pursuant to this subsection.

Page 14, after line 13, insert the following:

''(4) 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).''.

The Acting CHAIR. Pursuant to House Resolution 631, the gentleman from South Carolina (Mr. MULVANEY) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from South Carolina.

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

Madam Chair, I appreciate the opportunity to rise today to speak in favor to this amendment to the Cyber Intelligence Sharing and Protection Act. CISPA is fundamentally based on the authority granted to Congress in article I of the Constitution and article IV of the Constitution, specifically to provide for the common defense and to protect the Nation against invasion—in fact, the only affirmative duty that this government is obligated to meet under the terms of our Constitution.

This bill protects our Nation from foreign cyberthreats through the voluntary sharing of cyberthreat information. It is important for Members to understand this bill allows for only voluntary sharing of information on cybersecurity threats to the United States between the government and the private sector.

□ 1610

It includes no mandates to the private sector. It contains no new spending and strictly limits how the government can use the information that is voluntarily provided by the private sector. The amendment that I've offered with Mr. DICKS today goes one step further to protect the private information of American citizens. It explicitly prohibits the Federal Government from retaining or using the information for purposes other than specifically specified or set forth in the legislation.

Let's make it clear. The government cannot keep or use the shared information to see if you failed to pay your taxes. The government cannot use this information to read your emails. The government cannot use this information to track your credit card purchases or look at the Web sites that you've been visiting. Under our amendment, the Federal Government cannot use retained information unless it was directly related to a cyber or national security threat.

Finally, this bipartisan amendment requires—requires—the Federal Government to notify any private sector entity that shares information with the government if that information is not, in fact, cyberthreat information so that it doesn't happen again, and the government must delete that information.

The privacy of American citizens is simply too important to dismiss. Our amendment narrows the scope of the bill to ensure personal information is protected and that we are focusing on the true threat—advanced, foreign state-sponsored cyberattacks against America and its private entities.

With that, I would yield such time as he may consume to the chairman.

Mr. ROGERS of Michigan. Madam Chair, I just want to rise in strong support of this amendment. I appreciate Mr. MULVANEY's working with the committee.

This is a limiting amendment, and I think it, again, is in response to making sure that the intent of the bill meets the language of the bill, and this is well done to continue to protect privacy and civil liberties of all Americans and still allow for the government to share malicious source code with the private sector.

Mr. RUPPERSBERGER. Madam Chair, I rise in opposition to the amendment; although I do not oppose the amendment.

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

There was no objection.

Mr. RUPPERSBERGER. I also support this amendment. It is very important. It's another example of what we're attempting to do to protect the privacy and civil liberties of our citizens but yet have a bill that we clearly need to protect them from a national security perspective.

I yield back the balance of my time.

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

The Acting CHAIR. The question is on the amendment offered by the gentleman from South Carolina (Mr. MULVANEY).

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

Mr. MULVANEY. Madam Chair, I demand a recorded vote.

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

AMENDMENT NO. 9 OFFERED BY MR. FLAKE

The Acting CHAIR. It is now in order to consider amendment No. 9 printed in House Report 112–454.

Mr. FLAKE. I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 12, after line 18, insert the following new subparagraph:

''(E) a list of the department or agency receiving such information;

The Acting CHAIR. Pursuant to House Resolution 631, the gentleman from Arizona (Mr. FLAKE) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Arizona.

Mr. FLAKE. This amendment is straightforward. It would require the inspector general of the intelligence community to include a list of federal agencies and departments receiving information shared with the government in the report already required by the underlying legislation.

This act is an important piece of legislation that will help private entities and utilities protect themselves from catastrophic attacks to their networks by creating the authority for private entities and utilities to voluntarily share information pertaining to cyberattacks with the Federal Government and vice versa.

H.R. 3523 avoids placing costly mandates on private industry and the creation of a new regulatory structure. That's what I really appreciate about this legislation, as I'm sure everyone does—it's voluntary.

As with any new intelligence program, however, it's incumbent on us to make sure robust protections exist to safeguard privacy rights. The inspector general report required under H.R. 3523 will provide a thorough review of the information shared under these new authorities and will address any impacts such sharing has on privacy and civil liberties. Adding the list of the departments and agencies that were recipients of this shared information, as my amendment would do, would add information on which government agencies exactly are receiving shared information. Such information will further mitigate the risk of abuse to privacy rights and increase the effectiveness of the inspector general's report.

I commend my colleagues from Michigan and Maryland. They've been working hard to put together this bipartisan measure, working up until the very last minute to ensure that Members' concerns are addressed, and I believe that this is an important piece of legislation.

I'd like to yield to the gentleman from Michigan such time as he may consume.

Mr. ROGERS of Michigan. I want to thank the gentleman from Arizona for working with us. This, again, was a negotiated amendment. The gentleman approached us with concerns to make sure that the IG report adequately reflected and allowed us to perform the adequate oversight. This amendment does that. I appreciate his work and effort, and I think this strengthens the bill and continues to provide the oversight and protection of civil liberties and privacy for all Americans.

The Acting CHAIR. Does any Member seek recognition in opposition?

Mr. FLAKE. I just want to say I support the legislation in the underlying bill, and I would urge support for this amendment as well, and I yield back the balance of my time.

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

The amendment was agreed to.

AMENDMENT NO. 11 OFFERED BY MR. POMPEO

The Acting CHAIR. It is now in order to consider amendment No. 11 printed in House Report 112–454.

Mr. POMPEO. Madam Chair, I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 14, after line 13, insert the following: ''(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.''.

The Acting CHAIR. Pursuant to House Resolution 631, the gentleman from Kansas (Mr. POMPEO) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Kansas.

Mr. POMPEO. Madam Chairman, I appreciate this opportunity to offer a second amendment to this incredibly important piece of legislation that's been worked on for an awfully long time to balance the security needs of our Nation and the privacy rights of every United States citizen.

Similar to the first amendment I offered, this amendment addresses some of the concerns raised by me, privacy folks, and civil libertarian advocates to make very clear the intentions of this legislation. I talked earlier about the threat we face today. It's real, it's foreign, it's domestic, and these cyberattacks are an enormous risk to our national security and to our economic security.

I now strongly support this legislation. I've had a chance to work with Chairman ROGERS and Ranking Member RUPPERSBERGER to solidify limitations on this legislation that make it very clear that this government's use of this information will be limited.

I think some have claimed incorrectly that the current bill could be read to provide new authority to the Federal Government to install its Einstein system on private sector networks and to monitor traffic and send it back to the government with absolutely no limitations. That's wrong.

This amendment, however, makes it even more clear. This amendment makes clear that nothing in this bill would alter existing authorities or provide any new authority to any entity to use a Federal Government-owned or -operated cybersecurity system on a private sector system or network to protect such a system or network.

Again, I'm pleased to support the legislation. It doesn't create any new regulatory regime. It doesn't create any more Federal bureaucracy. And it has no additional spending. I urge my colleagues to support this amendment and final passage of CISPA.

I yield whatever time he might consume to the chairman of the Intelligence Committee.

Mr. ROGERS of Michigan. This is an important amendment, and again, I think it alleviates some of the concerns. They were misguided, but this locks it down, makes it very tight and makes it very clear on the limiting of this information, which is the intent of this bill. So I think this amendment addresses the privacy and civil liberties advocates' claims that the liability protection in the bill with respect to the use of cybersecurity systems could be read to be broader than the activities authorized by the legislation.

As I said, that was not true, certainly not the intent. This amendment makes that very clear in the bill that that would not be its purpose, and it is a limiting amendment. I strongly support this amendment. It is a bipartisan amendment as well.

Mr. POMPEO. Madam Chairwoman, I yield back the balance of my time.

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

The amendment was agreed to.

□ 1620

AMENDMENT NO. 12 OFFERED BY MR. WOODALL

The Acting CHAIR. It is now in order to consider amendment No. 12 printed in House Report 112–454.

Mr. WOODALL. Madam Chair, I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 14, after line 13 insert the following: ''(4) 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.

The Acting CHAIR. Pursuant to House Resolution 631, the gentleman

from Georgia (Mr. WOODALL) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Georgia.

Mr. WOODALL. Madam Chair, my amendment is a simple amendment. What we're doing here in this bill today, to the great credit of the chairman and the ranking member, is instituting a voluntary system by which our private companies and utilities can cooperate in the name of securing America's cyberspace. But what happens so often is, when the Federal Government creates a so-called ''voluntary'' standard, suddenly those folks who choose not to play on that playing field are subject to new liabilities because they rejected that voluntary standard.

Well, if it's going to be a truly voluntary standard, we have to ensure that those who reject it are not held to any new liabilities. I believe that was the intent of the committee as they crafted this legislation, but my amendment makes that clear to say that no new liabilities arise for any company that chooses not to participate in this new truly voluntary cybersecurity cooperative regime.

With that, I reserve the balance of my time.

The Acting CHAIR. Does any Member seek recognition in opposition?

Mr. WOODALL. With that, I want to thank the ranking member and the chairman for their tremendous openness throughout this entire process. Briefing after briefing, phone call after phone call, they both made themselves available to Members on both sides of the aisle so that we could get our questions answered in what is sometimes a difficult area to understand and digest. I thank them both for their leadership, and I yield back the balance of my time.

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

The amendment was agreed to.

AMENDMENT NO. 13 OFFERED BY MR. GOODLATTE

The Acting CHAIR. It is now in order to consider amendment No. 13 printed in House Report 112–454.

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

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 14, after line 14 insert the following:

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

Page 15, strike lines 1 through 25 and insert the following:

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

''(3) 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;

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

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

''(iv) efforts to gain unauthorized access to a system or network of a government or private entity, 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.

''(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 that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

''(4) 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;

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

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

''(iv) efforts to gain unauthorized access to a system or network of a government or private entity, 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.

''(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 that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

Page 16, strike line 5 and all that follows through page 17, line 2, and insert the following:

''(5) 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 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.

''(6) 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 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.

Page 17, after line 2 insert the following:

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

The Acting CHAIR. Pursuant to House Resolution 631, the gentleman from Virginia (Mr. GOODLATTE) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Virginia.

Mr. GOODLATTE. Madam Chair, I rise to offer an amendment to H.R. 3523. This amendment is the result of a series of long discussions between Members of the bipartisan coalition supporting this bill and various privacy and civil liberties groups.

As many know, I have long worked with these outside groups and with industry to make sure that where Congress acts with respect to technology, it does so in a way that is thoughtful, intelligent, and shows a strong respect for privacy and civil liberties.

I am a firm believer that Congress can craft legislation that addresses technology issues and allows the private sector to flourish while also protecting the rights of Americans. This amendment seeks to move the legislation further down that path.

To do so, this amendment carefully narrows the definitions of the key terms in the bill—''cyberthreat information,'' ''cyberthreat intelligence,'' ''cybersecurity purposes,'' and ''cybersecurity systems''—and adds in three new definitions from the existing law. Together, these new definitions ensure that companies in the private sector can protect themselves against very real cyberthreats. At the same time, they limit what information the private sector can identify, obtain, and share with others, and they do so in a way that is technology neutral so that the definitions we write into law today do not become obsolete before the ink is dry.

Specifically, these new definitions remove language from prior versions of the bill that could have been interpreted in broad ways. They remove or modify definitions that could have

been thought to cover things that the bill did not intend to cover, like unauthorized access to a system or network that purely involves violations of a terms of service. These revised definitions also rely in part on existing law to cover the appropriate set of threats to networks and systems without being overly broad.

I would note that these definitional changes are important on their own for the narrowing function they serve. In the view of groups like the Center for Democracy and Technology and the Constitution Project, this amendment represents ''important privacy improvement.'' Specifically, the change to the definitions addresses a number of key issues raised by a variety of groups, and many in the Internet user community. As such, these amendments move an already important bill in an even better direction.

I reserve the balance of my time.

Mr. RUPPERSBERGER. Madam Chairman, I rise in opposition to the amendment, but I do not oppose the amendment.

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

There was no objection.

Mr. RUPPERSBERGER. I yield 1 minute to the gentleman from Texas (Mr. POE).

Mr. POE of Texas. I thank the gentleman for yielding.

Anytime the government gets involved in data sharing and data storage, there is going to be the possibility for abuse.

I hear from my constituents in Texas and U.S. companies that they continue to lose information to cyberattacks from abroad. Most of these attacks come from none other than the organized crime syndicate of China, as I call it. They steal our intellectual property, and then they use the stolen information to compete against the United States.

We need a commonsense information-sharing system to combat the growing threat to this way of life that we have in America. However, we have to do it in such a way that protects our privacy and constitutional rights of citizens.

While I believe the intent of the base bill was never to allow the government to use information it obtained for any other purposes than cybersecurity, I believe that the clear and simple language in Mr. GOODLATTE's amendment is necessary to make it 100 percent clear that this is strictly prohibited.

As we remember from the 2012 NDAA debate, it's important, especially when dealing with legislation that affects civil liberties and constitutional rights, Congress needs to be perfectly 100 percent clear. I believe the Goodlatte amendment does this. I urge all Members to support it.

Mr. GOODLATTE. Madam Chairman, at this time, I am pleased to yield 1 minute to the chairman of the Intelligence Committee, the gentleman from Michigan (Mr. ROGERS).

Mr. ROGERS of Michigan. I want to thank the distinguished former chairman and member, Mr. GOODLATTE, for his commonsense amendment. Again, this is working to make sure that this bill is restricted for both information use, privacy, and civil liberties, and why the coalition, I argue, continues to grow because of the good work of folks like Mr. GOODLATTE. It's bipartisan in nature, and I would strongly urge the body's support for the Goodlatte amendment.

Mr. GOODLATTE. Madam Chairman, I am not aware of any other speakers on this amendment, so I would urge my colleagues to support the amendment. It is, as the chairman indicated and the ranking member indicated, bipartisan legislation that will improve the underlying bill in significant ways and protect the civil liberties of American citizens in a more clear fashion.

I thank all of those in the Chamber and outside who contributed ideas to help us craft this amendment and urge all of my colleagues to support it.

I yield back the balance of my time.

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

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

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

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

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. WOODALL) having assumed the chair, Mrs. CAPITO, Acting Chair of the Committee of the Whole House on the state of the Union, reported that that Committee, having had under consideration the bill (H.R. 3523) 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.

Mr. ROGERS of Michigan. Mr. Speaker, I ask unanimous consent that during further consideration of H.R. 3523, pursuant to House Resolution 631, amendments No. 10 and No. 5 in House Report 112–454 may be considered out of sequence.

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 631 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. 3523.

Will the gentlewoman from West Virginia (Mrs. CAPITO) kindly resume the chair.

□ 1630

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. 3523) 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 Mrs. CAPITO (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. 13 printed in House Report 112–454 by the gentleman from Virginia (Mr. GOODLATTE) had been postponed.

AMENDMENT NO. 14 OFFERED BY MR. TURNER OF OHIO

The Acting CHAIR. It is now in order to consider amendment No. 14 printed in House Report 112–454.

Mr. TURNER of Ohio. Madam Chair, I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 15, line 7, insert ''deny access to or'' before ''degrade''.

Page 15, line 20, insert ''deny access to or'' before ''degrade''.

Page 16, line 10, insert ''deny access to or'' before ''degrade''.

Page 16, line 21, insert ''deny access to or'' before ''degrade''.

The Acting CHAIR. Pursuant to House Resolution 631, the gentleman from Ohio (Mr. TURNER) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Ohio.

Mr. TURNER of Ohio. Madam Chairman, this amendment would make a technical correction to the definition sections of this bill to ensure that U.S. cybersecurity policies remain consistent for protections against threats to our government and private sector networks.

This amendment will maintain consistency among this bill and other cybersecurity policies. The terms ''deny, degrade, disrupt or destroy'' are found throughout our national cybersecurity strategy and our guidance documents. The term ''deny'' was inadvertently omitted from H.R. 3523. Inserting ''deny'' makes the bill consistent with other national documents in the discussion of cybersecurity.

The increase in cybersecurity incidents led to the development of centers like the Air Force's Cyberspace Technical Center of Excellence at Wright Patterson Air Force base in my district in Dayton, Ohio. To combat this growing trend in the sophistication of cyberattacks, the Center of Technical Excellence has been turned to that focus.

The need to protect U.S. networks from denial-of-service attacks was made clear when, for 3 weeks in 2007, Estonia was the target of a large-scale

series of denial-of-service attacks against government Web sites, banks, universities, and Estonian newspapers.

I urge all of my colleagues to support this amendment and the underlying bill.

I yield 30 seconds to the chairman.

Mr. ROGERS of Michigan. Madam Chair, I want to, again, thank Mr. TURNER for this important clarification amendment and working with us to improve the status of the bill to make sure that we are able to protect America's networks and increases the ability for us to protect privacy and civil liberties.

I appreciate the gentleman's good effort, and I would encourage the House to support the Turner amendment.

The Acting CHAIR. Does any Member seek recognition in opposition?

Mr. TURNER of Ohio. Madam Chair, I yield back the balance of my time.

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

The amendment was agreed to.

AMENDMENT NO. 15 OFFERED BY MR. MULVANEY

The Acting CHAIR. It is now in order to consider amendment No. 15 printed in House Report 112–454.

Mr. MULVANEY. Madam Chair, I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

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

SEC. 3. SUNSET.

Effective on the date that is five 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 Acting CHAIR. Pursuant to House Resolution 631, the gentleman from South Carolina (Mr. MULVANEY) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from South Carolina.

Mr. MULVANEY. This amendment, ladies and gentlemen, is fairly simple and straightforward, but it bears discussion for a few moments. It requires the bill to expire of its own terms within 5 years. It's what we call in this business a sunset clause. And by its own terms, if the bill is passed, it will automatically cease to be, cease to be enforceable after 5 years unless this body acts affirmatively to renew it.

Generally, I think this is good policy with most things that we do in Washington, D.C. In fact, several people say that one of the biggest difficulties we have in this town is that we simply create laws all the time and they never go away. So generally speaking, I think sunset clauses are to be admired and to be encouraged.

Even more so is the case, however, when we deal with situations where we have concerns regarding individual liberties. We've worked very, very hard to make this bill a good bill. It is an excellent bill. I'm proud to be a cosponsor of this bill.

But every single time that we start moving into the realm where the government action starts to bump up against individual liberties, it's a good idea to take a pause after this certain amount of time, in this case 5 years, and look our hands over, look over the actual implementation of the bill and make sure that we did exactly what we thought that we were going to do.

Finally, I think in a case when we're dealing with technology, which moves so very rapidly—in fact, we've written this bill as well as we possibly could to try and deal with unanticipated development in technology—but when you're dealing with technology that moves so rapidly and changes so quickly, I think it's important, after a certain period of time, again, here, 5 years, to step back, look our hands over and make sure that things worked exactly as we thought they would.

So, for that reason, Madam Chairman, I ask that this amendment be considered and be approved.

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

The Acting CHAIR. Does any Member seek recognition in opposition to the Member's amendment?

The question is on the amendment offered by the gentleman from South Carolina (Mr. MULVANEY).

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

Mr. MULVANEY. Madam Chair, I demand a recorded vote.

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

AMENDMENT NO. 5 OFFERED BY MS. JACKSON LEE OF TEXAS

The Acting CHAIR. It is now in order to consider amendment No. 5 printed in House Report 112–454.

Ms. JACKSON LEE of Texas. Madam Chair, I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 9, after line 5, insert the following:

''(c) CYBERSECURITY OPERATIONAL ACTIVITY.—

''(1) IN GENERAL.—In receiving information authorized to be shared with the Federal Government under this section, the Secretary of Homeland Security is authorized, notwithstanding any other provision of law, to acquire, intercept, retain, use, and disclose communications and other system traffic that are transiting to or from or stored on Federal systems and to deploy countermeasures with regard to such communications and system traffic for cybersecurity purposes provided that the Secretary certifies that—

''(A) such acquisitions, interceptions, and countermeasures are reasonable necessary for the purpose of protection Federal systems from cybersecurity threats;

''(B) the content of communications will be collected and retained only when the communication is associated with known or reasonably suspected cybersecurity threat, and communications and system traffic will not be subject to the operation of a countermeasure unless associated with such threats;

''(C) information obtained pursuant to activities authorized under this subsection will only be retained, used or disclosed to protect Federal systems from cybersecurity threats, mitigate against such threats, or, with the approval of the Attorney General, for law enforcement purposes when the information is evidence of a crime which has been, is being, or is about to be committed; and

''(D) notice has been provided to users of Federal systems concerning the potential for acquisition, interception, retention, use, and disclosure of communications and other system traffic.

''(2) CONTRACTS.— The Secretary may enter into contracts or other agreements, or otherwise request and obtain the assistance of, private entities that provide electronic communication or cybersecurity services to acquire, intercept, retain, use, and disclose communications and other system traffic consistent with paragraph (1).

''(3) PRIVILEGED COMMUNICATIONS.—No otherwise privileged communication obtained in accordance with, or in violation of, this section shall lose its privileged character.

''(4) POLICIES AND PROCEDURES.— The Secretary of Homeland Security shall establish policies and procedures that—

''(A) minimize the impact on privacy and civil liberties, consistent with the need to protect Federal systems and critical information infrastructure from cybersecurity threats and mitigate cybersecurity threats;

''(B) reasonably limit the acquisition, interception, retention, use, and disclosure of communications, records, system traffic, or other information associated with specific persons consistent with the need to carry out the responsibilities of this section, including establishing a process for the timely destruction on recognition of communications, records, system traffic, or other information that is acquired or intercepted pursuant to this section that does not reasonably appear to be related to protecting Federal systems and critical information infrastructure from cybersecurity threats and mitigating cybersecurity threats;

''(C) include requirements to safeguard communications, records, system traffic, or other information that can be used to identify specific persons from unauthorized access or acquisition; and

''(D) protect the confidentiality of disclosed communications, records, system traffic, or other information associated with specific persons to the greatest extent practicable and require recipients of such information to be informed that the communications, records, system traffic, or other information disclosed may only be used for protecting information systems against cybersecurity threats, mitigating against cybersecurity threats, or law enforcement purposes when the information is evidence of a crime that has been, is being, or is about to be committed, as specified by the Secretary.

Page 14, after line 24, insert the following:

''(2) COUNTERMEASURE.—The term 'countermeasure' means an automated action with defensive intent to modify or block data packets associated with electronic or wire communications, internet traffic, program code, or other system traffic transiting to or from or stored on an information system to counteract a cybersecurity threat.''.

The Acting CHAIR. Pursuant to House Resolution 631, the gentlewoman from Texas (Ms. JACKSON LEE) and a

Member opposed each will control 5 minutes.

The Chair recognizes the gentlewoman from Texas.

Ms. JACKSON LEE of Texas. Madam Chair, let me thank you for your courtesy. Let me thank the chairperson for his courtesy and the ranking member for his courtesy. I was very appreciative, with the overlapping committee work, for the courtesy of the floor. I thank you very much.

Let me hold up the Constitution and say that I believe in the Constitution and the Bill of Rights, particularly, that protects us against unreasonable search and seizure. And I also recognize the bipartisan effort of this particular legislation and recognize that we may have disagreement.

My amendment ensures that comprehensive policies and procedures are implemented by the Department of Homeland Security to protect Federal systems from cybersecurity threats and minimize the impact on privacy. What it does not do is allow Homeland Security and the Justice Department to spy on Americans.

Let me be very clear. It does not allow the infrastructure of Homeland Security and the Justice Department to spy on Americans. I would not adhere to that.

It is a shame that oversight of our Nation's critical infrastructure, however, was not included in this bill. The hard work that has been done by the Committee on Homeland Security, Mr. LUNGREN and Ms. CLARKE, joined with other Members, was worthy of consideration.

I understand the strictures that we're dealing with. My amendment is designed to put in place comprehensive privacy protections in order to prevent any gross infringement of an individual's civil liberties or privacy rights. It allows the Department of Homeland Security to protect Federal systems that enable air traffic controllers to operate.

Madam Chairperson, we know the climate that we live in. God has blessed us, if I might even say that, but more importantly, the hard work of men and women who happen to be Federal employees, that no action has occurred on our soil since 9/11.

This amendment would allow the Department of Homeland Security to protect Federal systems that enable air traffic controllers to operate, that enable Congress to operate, that enable all Federal agencies to operate.

My amendment is intentionally narrowly tailored to go after known or reasonable threats to our Federal systems. Let me be very clear. This is not a reflection on this legislation from the extent of hard work.

□ 1640

I am just saying that, coming from my perspective, I would hope that we would look at infrastructure.

I am not advocating for the bill. I am advocating for an open discussion on this issue that certain elements have to be resolved in dealing with the cyberthreats that we face. I've long been an advocate for protecting the right to privacy and the civil liberties of all Americans—that is very much a part of this amendment—but I am also mindful of the importance of the infrastructure.

As we assess cybersecurity measures and take steps to implement legislation, I believe we must be sure to strike the proper balance between effective and strong security for our digital networks and protecting the privacy of individuals as well as infrastructure that involves transportation. I am ever mindful that we must be careful not to go about strengthening cybersecurity at the expense of infringing on people's privacy rights and civil liberties, which is why my amendment is narrowly tailored and sets clear restrictions on the scope of communications addressed and why and how that information can be used.

Our Nation's critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials.

I ask my colleagues to support the amendment, and I reserve the balance of my time.

Mr. ROGERS of Michigan. I rise in opposition to the amendment.

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

Mr. ROGERS of Michigan. I yield myself 1½ minutes.

If you thought it was good for the businesses to require Facebook to give them your passwords, you'll love this. If not, you should go apoplectic. I think that's an awful practice on Facebook. This is worse. I want to read just from the law. Notwithstanding any other provision, it allows them to:

> acquire, intercept, retain, use, and disclose communications and other system traffic that are transiting to and from or are stored on the Federal systems and to deploy countermeasures with regard to such communications and system traffic for cybersecurity purposes.

This is dangerous. It's dangerous. For the very narrow bill that has been misrepresented from what we do, this is Big Brother on steroids. We cannot allow this to happen. This would be the government tracking communications or your medical records from the veterans' association. It would track your IRS forms coming in and out of the Federal Government. This is exactly what scares people about trying to get into the business of making sure we protect our networks, but we can't do it by trampling on privacy and civil liberties.

This is awful. I am just shocked, after all of this debate and all of this discussion on our very narrow bill, that my friends would come up with something that wholesale monitors the Internet and gets all of the information which we've fought so hard to protect on behalf of average Americans.

I yield 2 minutes to the gentleman from Georgia (Mr. WESTMORELAND).

Mr. WESTMORELAND. I want to thank the chairman for yielding.

Let me say this to my colleague from Texas: that we have had a number of amendments here today that have tried to streamline this bill in order to make it even narrower and to take out any perception that it would be personal information and limit what government can do and be very explicit in the terms of what this sharing is, which is voluntary, which is narrowly drawn.

The chairman and the ranking member have done a wonderful job of working with other Members to allow these amendments to make this bill better. I am very disappointed. This amendment basically guts the bill—it expands it—when everybody who has been down here so far has been trying to narrow it. This just expands it even more. This is the type of amendment that people fear in that we would give Homeland Security the ability to intercept and keep the transmissions. That is totally out of hand.

I just hope that we will vote against this amendment and support the underlying bill.

Ms. JACKSON LEE of Texas. What an exaggeration. I know that they have been propelled by all of the media that has given them great support.

They know that the underlying bill, in fact, is considered an invasion of privacy; but if you look at my amendment, it is only when the communication is associated with a known or a reasonably suspected cybersecurity threat. It is narrow, but more importantly, it has a privacy provision. I believe in privacy. Let me just say that I was not going to be denied the right to come to the floor to be able to frame what we should be doing—looking at infrastructure and the complement of making sure that privacy is protected.

This particular book, even with the amendments they have, will probably not draw this to the point of acceptance. So I would argue that this is a productive debate but that the amendment that Jackson Lee has submitted does not, in fact, at all violate privacy. I would say to them that I look forward to being able to address this question as we go forward.

I am going to ask, at this time, unanimous consent to withdraw this amendment for the misinterpretation that my friends on the other side of the aisle have predicted or thought that they were going to put on this particular amendment.

The Acting CHAIR. Without objection, the amendment is withdrawn.

There was no objection.

AMENDMENT NO. 10 OFFERED BY MS. RICHARDSON

The Acting CHAIR. It is now in order to consider amendment No. 10 printed in House Report 112–454.

Ms. RICHARDSON. Madam Chairwoman, I have an amendment at the desk.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 14, after line 6, insert the following new subparagraph:

''(C) prohibit a department or agency of the Federal Government from providing cyber threat information to owners and operators of critical infrastructure;

The Acting CHAIR. Pursuant to House Resolution 631, the gentlewoman from California (Ms. RICHARDSON) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentlewoman from California.

Ms. RICHARDSON. I stand today in support of the Richardson amendment to H.R. 3523; but I would like to take a moment to thank the majority leader, Mr. CANTOR, Chairman ROGERS, and Ranking Member RUPPERSBERGER for their tolerance in allowing us to come to the floor. I was ranking member of a committee that was in operation at this time, and I thank you for allowing us to come forward.

The Richardson amendment ensures that owners and operators of critical infrastructure systems that are potential targets to cyberattacks receive information about cyberthreats. Some examples of our critical infrastructure systems that this amendment would apply to are: energy facilities, banking and finance facilities, chemical facilities, dams, nuclear plants, emergency services, agriculture and food systems, water treatment systems. Many of these would be in great danger and would need information.

Every single Member of Congress has critical infrastructure sectors in their districts, whether they be public or private, and every community in this Nation has some critical infrastructure presence that should be protected and advised of threats. In my district, I have the Home Depot Athletic Center, which holds up to 27,000 people. There is the Boeing Company, which manufactures the C–17 planes. There is the Long Beach Police and Fire Department EOC center, the Long Beach Gas and Oil Department, and water treatment facilities. The numbers go on. We need to make sure that not only ports and government facilities but also private facilities are approved and entitled to have this same information.

Some inherent complications are that there are 18 different Federal Government agencies that have jurisdiction over critical infrastructure sectors. For example, the Department of Homeland Security has jurisdiction over chemical, commercial facilities, dams, emergency services, and nuclear power alone.

H.R. 3523, as currently drafted, does not mention how critical infrastructure sectors that do not fall within the jurisdiction of government intelligence agencies would receive critical cyberthreat information or have the systems in place to share information appropriately. This amendment makes an important improvement to that legislation.

I would like to commend Chairman ROGERS and Ranking Member RUPPERSBERGER, who mentioned in their testimony before the Rules Committee and the Intelligence Committee that there was a key fault here in this critical infrastructure section. I am further pleased that the Rules Committee acknowledged that by finding this amendment in order, and I urge my colleagues to consider this seriously.

While Chairman LUNGREN's original cyber bill did not make it to the House floor, I offer this Richardson amendment in the same bipartisan spirit that I did when his bill was brought forward in our subcommittee. Mr. LUNGREN and Mr. LANGEVIN spoke earlier on the bipartisan amendment regarding critical infrastructure, hence my building my comments on that.

Richardson amendment No. 10 ensures that our critical infrastructure sectors will not be left out from receiving information that could protect their systems against a terrorist attack.

□ 1650

This amendment makes sure that industries most at risk of a cyberattack receive information that they need to protect the public and the facilities at large. My amendment makes explicit that critical infrastructure sectors be included in information-sharing relationships and does not include any new Federal authorities.

With that, Madam Chairwoman, I urge my colleagues to support the amendment.

Mr. ROGERS from Michigan. Madam Chair, I rise in opposition to the amendment.

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

Mr. ROGERS of Michigan. I appreciate the gentlelady's effort. Again, we were pretty careful in this year-long process of trying to find a very narrow solution because of all of the challenges that come with trying to get a piece of legislation across the House to the Senate to the President's desk.

I argue that the Homeland Security Committee should engage in a critical infrastructure debate. Here's the problem: it's not defined for the purposes of this bill. So we don't know what that means. We've been very careful to separate the government from the private sector. There is no government involvement in the private sector networks. It is just information, malicious source code-sharing. That's it.

This, we're not sure where it goes. Many in industry believe that they're talking about the backbone of the Internet. Are they talking about the backbone of the Internet? We don't know. It's not well defined. That would mean, then, that the government for the first time gets into the backbone of the Internet. I think that's a horrible, terrible idea.

So I don't think that's what the gentlelady intends, but the problem is that's not what the language says.

I look forward to working with the gentlelady as she works through those issues on Homeland Security because these are hard. They are tricky. Sometimes a word will get you in trouble, as we have found along the path here, and as it should. We should be really careful about how we're doing this.

So I would encourage the gentlelady to work with us. I know Mr. RUPPERSBERGER, since we've been through this, we can provide some help along the way, and we look forward to the product that you all work on that is geared toward the infrastructure piece. Again, this was never intended to solve all the problems. It was intended to be a very narrow first step to say, Hey, if your house is being robbed, we want to tell you before the robber gets there. That's all this bill does. It tells if your computer is going to get hacked and your personal information stolen, we want you to have the malicious code so you can protect yourself. That's all this bill does.

So we get a little nervous when it starts crossing that divide that we've established between the government and the private sector. You start crossing that divide, we think you can get into some serious trouble in a hurry without very clearly defined language and definition.

Unfortunately, I have to oppose the amendment, but I look forward to working with the gentlelady on a very important issue, infrastructure protection, as the Homeland Security does its work.

Mr. RUPPERSBERGER. Will the gentleman yield?

Mr. ROGERS of Michigan. I yield to the gentleman from Maryland.

Mr. RUPPERSBERGER. As we said before, our bill is extremely limited, and we're attempting again to allow our government, our intelligence community, to give the information that's necessary to protect our citizens from these cyberattacks.

Ours is the most active bill that is out there now. Our bill, hopefully, will pass and go to the Senate, and there will be a lot more negotiation. But there is a lot of work to do in other areas, too, such as Homeland Security; and I know there are other issues involved in the Homeland Security markup, I know that there are issues involving Judiciary.

I can say this: I know that the chairman and I for 1 year now have worked very openly with every group that we think would be involved in this bill. Because of different positions taken, including HLU, we listened. This bill is better, and we hope that it passes.

So we clearly will work with you, but we on the Intelligence Committee are very limited to our jurisdiction, and that's why a lot of these issues we can't deal with other than what is in our bill right now.

I thank the gentleman for yielding.

Ms. RICHARDSON. Again, I'd like to thank both the chairman and the ranking member and look forward to the opportunity to work with you.

I would just give you one analogy to consider as we move forward. As you recall on 9/11 when the planes hit those two Twin Towers, the government had the ability to notify the private airlines to scramble the planes and to demand that all of the planes would be landed because we didn't know where they were going to go.

At that point, the government had the ability to work with the private sector, with the airline industry, to communicate information that they were now becoming aware of.

I'm certainly not suggesting that we interfere with the free-flowing ideas of the Internet. What this amendment is suggesting, and I look forward to working with you in the future, is that the government does have the ability if in the event something happens with dropping some chemicals into water, for example, treatment facilities, that the government should certainly have the ability to work with those private sector companies to be able to notify them and ensure that the public is protected.

I thank you for hearing the amendment, and I look forward to working with you going forward.

I yield back the balance of my time.

Mr. ROGERS of Michigan. I thank the gentlelady, and I look forward to that opportunity.

I yield back the balance of my time.

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

The amendment was rejected.

ANNOUNCEMENT BY THE ACTING CHAIR

The Acting CHAIR. The Chair understands that amendment No. 16 will not be offered.

Pursuant to clause 6 of rule XVIII, proceedings will now resume on those amendments printed in House Report 112–454 on which further proceedings were postponed, in the following order:

Amendment No. 1 by Mr. LANGEVIN of Rhode Island.

Amendment No. 4 by Mr. ROGERS of Michigan.

Amendment No. 6 by Mr. QUAYLE of Arizona.

Amendment No. 7 by Mr. AMASH of Michigan.

Amendment No. 8 by Mr. MULVANEY of South Carolina.

Amendment No. 13 by Mr. GOODLATTE of Virginia.

Amendment No. 15 by Mr. MULVANEY of South Carolina.

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. LANGEVIN

The Acting CHAIR. The unfinished business is the demand for a recorded vote on the amendment offered by the gentleman from Rhode Island (Mr. LANGEVIN) on which further proceedings were postponed and on which the noes 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 167, noes 243, not voting 21, as follows:

[Roll No. 184]

AYES—167

Ackerman
Andrews
Baldwin
Bass (CA)
Becerra
Berkley
Berman
Bishop (GA)
Bishop (NY)
Bonamici
Boren
Boswell
Brady (TX)
Braley (IA)
Brown (FL)
Butterfield
Capps
Capuano
Carnahan
Carney
Carson (IN)
Castor (FL)
Chandler
Chu
Cicilline
Clarke (MI)
Clay
Cleaver
Clyburn
Coffman (CO)
Cohen
Connolly (VA)
Conyers
Cooper
Costa
Critz
Cuellar
Cummings
Davis (CA)
Davis (IL)
DeFazio
DeGette
DeLauro
Dent
Deutch
Dicks
Dingell
Doggett
Doyle
Edwards
Ellison
Engel
Farr
Fattah
Frank (MA)
Fudge
Garamendi
Gibson
Gonzalez
Green, Al
Grijalva
Grimm
Gutierrez
Hahn
Hanabusa
Hastings (FL)
Heinrich
Higgins
Himes
Hinchey
Hochul
Holt
Honda
Hoyer
Israel
Jackson (IL)
Jackson Lee (TX)
Johnson, E. B.
Kaptur
Keating
Kildee
Kind
King (NY)
Kissell
Kucinich
Langevin
Larsen (WA)
Larson (CT)
Lee (CA)
Levin
Lewis (GA)
Lipinski
Loebsack
Lofgren, Zoe
Lowey
Luján
Lungren, Daniel E.
Lynch
Markey
Matsui
McCollum
McDermott
McGovern
McIntyre
Meehan
Meeks
Michaud
Miller (NC)
Miller, George
Moore
Moran
Nadler
Neal
Olver
Owens
Pallone
Pascrell
Pastor (AZ)
Pelosi
Perlmutter
Peters
Pingree (ME)
Polis
Price (NC)
Quigley
Reyes
Richardson
Richmond
Rothman (NJ)
Roybal-Allard
Ruppersberger
Rush
Ryan (OH)
Sánchez, Linda T.
Sanchez, Loretta
Sarbanes
Schakowsky
Schiff
Schwartz
Scott (VA)
Serrano
Sewell
Shuler
Smith (WA)
Speier
Stark
Sutton
Thompson (CA)
Thompson (MS)
Thornberry
Tierney
Tonko
Towns
Tsongas
Turner (NY)
Van Hollen
Velázquez
Visclosky
Walz (MN)
Wasserman Schultz
Waters
Watt
Waxman
Wilson (FL)
Woodall
Woolsey
Yarmuth

NOES—243

Adams
Aderholt
Akin
Alexander
Altmire
Amash
Amodei
Austria
Baca
Bachmann
Bachus
Barletta
Barrow
Bartlett
Barton (TX)
Bass (NH)
Benishek
Berg
Biggert
Bilbray
Bilirakis
Bishop (UT)
Black
Blackburn
Bonner
Bono Mack
Boustany
Brady (PA)
Brooks
Broun (GA)
Buchanan
Buerkle
Burgess
Burton (IN)
Calvert
Camp
Campbell
Capito
Carter
Cassidy
Chabot
Chaffetz
Coble
Cole
Conaway
Costello
Courtney
Cravaack
Crawford
Crenshaw
Crowley
Culberson
Denham
DesJarlais
Diaz-Balart
Dold
Donnelly (IN)
Dreier
Duffy
Duncan (SC)
Duncan (TN)
Ellmers
Emerson
Eshoo
Farenthold
Fincher
Fitzpatrick
Flake
Fleischmann
Fleming
Flores
Forbes
Fortenberry
Foxx
Franks (AZ)
Frelinghuysen
Gallegly
Gardner
Garrett
Gerlach
Gibbs
Gingrey (GA)
Gohmert
Goodlatte
Gosar
Gowdy
Granger
Graves (GA)
Graves (MO)
Green, Gene
Griffin (AR)
Griffith (VA)
Guinta
Guthrie
Hall
Hanna
Harper
Harris
Hartzler
Hastings (WA)
Hayworth
Heck
Hensarling
Herger
Herrera Beutler
Hinojosa
Huelskamp
Huizenga (MI)
Hultgren
Hunter
Hurt
Issa
Jenkins
Johnson (IL)
Johnson (OH)
Johnson, Sam
Jones
Jordan
Kelly
King (IA)
Kingston
Kinzinger (IL)
Kline
Labrador
Lamborn
Lance
Landry
Lankford
Latham
LaTourette
Latta
Lewis (CA)
LoBiondo
Long
Lucas
Luetkemeyer
Lummis
Mack
Manzullo
Marchant
Matheson
McCarthy (CA)
McCarthy (NY)
McCaul
McClintock
McCotter
McKeon
McKinley
McMorris Rodgers
McNerney
Mica
Miller (FL)
Miller (MI)
Miller, Gary
Mulvaney
Murphy (PA)
Myrick
Napolitano
Neugebauer
Noem
Nugent
Nunes
Nunnelee
Olson
Palazzo
Paulsen
Pearce
Peterson
Petri
Pitts
Platts
Poe (TX)
Pompeo
Posey
Price (GA)
Quayle
Rahall
Reed
Rehberg
Reichert
Renacci
Ribble
Rigell
Rivera
Roby
Roe (TN)
Rogers (AL)
Rogers (KY)
Rogers (MI)
Rohrabacher
Rokita
Rooney
Ros-Lehtinen
Roskam
Ross (AR)
Ross (FL)
Royce
Runyan
Ryan (WI)
Scalise
Schilling
Schmidt
Schock
Schrader
Schweikert
Scott (SC)
Scott, Austin
Sensenbrenner
Sessions
Sherman
Shimkus
Shuster
Simpson
Smith (NE)
Smith (NJ)
Smith (TX)
Southerland
Stearns
Stivers
Stutzman
Sullivan
Terry
Thompson (PA)
Tiberi
Tipton
Turner (OH)
Upton
Walberg
Walden
Walsh (IL)
Webster
Welch
West
Westmoreland
Whitfield
Wilson (SC)
Wittman
Wolf
Womack
Yoder
Young (AK)
Young (FL)
Young (IN)

NOT VOTING—21

Blumenauer
Bucshon
Canseco
Cantor
Cardoza
Clarke (NY)
Davis (KY)
Filner
Hirono
Holden
Johnson (GA)
Maloney
Marino
McHenry
Murphy (CT)
Paul
Pence
Rangel
Scott, David
Sires
Slaughter

□ 1723

Messrs. ALEXANDER, COSTELLO, DUNCAN of South Carolina, REHBERG, COURTNEY and PEARCE changed their vote from ''aye'' to ''no.''

Mr. BRADY of Texas, Ms. SEWELL, Ms. LORETTA SANCHEZ of California, Mr. CONYERS, Ms. WATERS, Ms. MCCOLLUM and Ms. PINGREE of Maine changed their vote from ''no'' to ''aye.''

So the amendment was rejected.

The result of the vote was announced as above recorded.

Stated for:

Mr. FILNER. Mr. Chair, on rollcall 184, I was away from the Capitol due to prior commitments to my constituents. Had I been present, I would have voted ''aye.''

AMENDMENT NO. 4 OFFERED BY MR. ROGERS OF MICHIGAN

The Acting CHAIR (Mr. CHAFFETZ). 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 Acting CHAIR. This will be a 2-minute vote.

The vote was taken by electronic device, and there were—ayes 412, noes 0, not voting 19, as follows:

[Roll No. 185]

AYES—412

Ackerman
Adams
Aderholt
Akin
Alexander
Altmire
Amash
Amodei
Andrews
Austria
Baca
Bachmann
Bachus
Baldwin
Barletta
Barrow
Bartlett
Barton (TX)
Bass (CA)
Bass (NH)
Becerra
Benishek
Berg
Berkley
Berman
Biggert
Bilbray
Bilirakis
Bishop (GA)
Bishop (NY)
Bishop (UT)
Black
Blackburn
Bonamici
Bonner
Bono Mack
Boren
Boswell
Boustany
Brady (PA)
Brady (TX)
Braley (IA)
Brooks
Broun (GA)
Brown (FL)
Buchanan
Buerkle
Burgess
Burton (IN)
Butterfield
Calvert
Camp
Campbell
Cantor
Capito
Capps
Capuano
Cardoza
Carnahan
Carney
Carson (IN)
Carter
Cassidy
Castor (FL)
Chabot
Chaffetz
Chandler
Chu
Cicilline
Clarke (MI)
Clay
Cleaver
Clyburn
Coble
Coffman (CO)
Cohen
Cole
Conaway
Connolly (VA)
Conyers
Cooper
Costa
Costello
Courtney
Cravaack
Crawford
Crenshaw
Critz
Crowley
Cuellar
Culberson
Cummings
Davis (CA)
Davis (IL)
DeFazio
DeGette
DeLauro
Denham
Dent
DesJarlais
Deutch
Diaz-Balart
Dicks
Dingell
Doggett
Dold
Donnelly (IN)
Doyle
Dreier
Duffy
Duncan (SC)
Duncan (TN)
Edwards
Ellison
Ellmers
Emerson
Engel
Eshoo
Farenthold
Farr
Fattah
Fincher
Fitzpatrick
Flake
Fleischmann
Fleming
Flores
Forbes
Fortenberry
Foxx
Frank (MA)
Franks (AZ)
Frelinghuysen
Fudge
Gallegly
Garamendi
Gardner
Garrett
Gerlach
Gibbs
Gibson
Gingrey (GA)
Gohmert
Gonzalez
Goodlatte
Gosar
Gowdy
Granger
Graves (GA)
Graves (MO)
Green, Al
Green, Gene
Griffin (AR)
Griffith (VA)
Grijalva
Grimm
Guinta
Guthrie
Gutierrez
Hahn
Hall
Hanabusa
Hanna
Harper
Harris
Hartzler
Hastings (FL)
Hastings (WA)
Hayworth
Heck
Heinrich
Hensarling
Herger
Herrera Beutler
Higgins
Himes
Hinchey
Hinojosa
Hochul
Holt
Honda
Hoyer
Huelskamp
Huizenga (MI)
Hultgren
Hunter
Hurt
Israel
Issa
Jackson (IL)
Jackson Lee (TX)
Jenkins
Johnson (IL)
Johnson (OH)
Johnson, E. B.
Johnson, Sam
Jones
Jordan
Kaptur
Keating
Kelly
Kildee
Kind
King (IA)
King (NY)
Kingston
Kinzinger (IL)
Kissell
Kline
Kucinich
Labrador
Lamborn
Lance
Langevin
Lankford
Larsen (WA)
Larson (CT)
Latham
LaTourette
Latta
Lee (CA)
Levin
Lewis (CA)
Lewis (GA)
Lipinski
LoBiondo
Loebsack
Lofgren, Zoe
Long
Lowey
Lucas
Luetkemeyer
Luján
Lummis
Lungren, Daniel E.
Lynch
Mack
Manzullo
Marchant
Markey
Matheson
Matsui
McCarthy (CA)
McCarthy (NY)
McCaul
McClintock
McCollum
McCotter
McDermott
McGovern
McIntyre
McKeon
McKinley
McMorris Rodgers
McNerney
Meehan
Meeks
Mica
Michaud
Miller (FL)
Miller (MI)
Miller (NC)
Miller, Gary
Miller, George
Moore
Moran
Mulvaney
Murphy (CT)
Murphy (PA)
Myrick
Nadler
Napolitano
Neal
Neugebauer
Noem
Nugent
Nunes
Nunnelee
Olson
Olver
Owens
Palazzo
Pallone
Pascrell
Pastor (AZ)
Paulsen
Pearce
Pelosi
Perlmutter
Peters
Peterson
Petri
Pingree (ME)
Pitts
Platts
Poe (TX)
Polis
Pompeo
Posey
Price (GA)
Price (NC)
Quayle
Quigley
Rahall
Reed
Rehberg
Reichert
Renacci
Reyes
Ribble
Richardson
Richmond
Rigell
Rivera
Roby
Roe (TN)
Rogers (AL)
Rogers (KY)
Rogers (MI)
Rohrabacher
Rokita
Rooney
Ros-Lehtinen
Roskam
Ross (AR)
Ross (FL)
Rothman (NJ)
Roybal-Allard
Royce
Runyan
Ruppersberger
Rush
Ryan (OH)
Ryan (WI)
Sánchez, Linda T.
Sanchez, Loretta
Sarbanes
Scalise
Schakowsky
Schiff
Schilling
Schmidt
Schock
Schwartz
Schweikert
Scott (SC)
Scott (VA)
Scott, Austin
Scott, David
Sensenbrenner
Serrano
Sessions
Sewell
Sherman
Shimkus
Shuler
Shuster
Simpson
Smith (NE)
Smith (NJ)
Smith (TX)
Smith (WA)
Southerland
Speier
Stark
Stearns
Stivers
Stutzman
Sullivan
Sutton
Terry
Thompson (CA)
Thompson (MS)
Thompson (PA)
Thornberry
Tiberi
Tierney
Tipton
Tonko
Towns
Tsongas
Turner (NY)
Turner (OH)
Upton
Van Hollen
Velázquez
Visclosky
Walberg
Walden
Walsh (IL)
Walz (MN)
Wasserman Schultz
Waters
Watt
Waxman
Webster
Welch
West
Westmoreland
Whitfield
Wilson (FL)
Wilson (SC)
Wittman
Wolf
Womack
Woodall
Woolsey
Yarmuth
Yoder
Young (AK)
Young (FL)
Young (IN)

NOT VOTING—19

Blumenauer
Bucshon
Canseco
Clarke (NY)
Davis (KY)
Filner
Hirono
Holden
Johnson (GA)
Landry
Maloney
Marino
McHenry
Paul
Pence
Rangel
Schrader
Sires
Slaughter

□ 1727

Mr. CUMMINGS changed his vote from ''no'' to ''aye.''

So the amendment was agreed to.

The result of the vote was announced as above recorded.

Stated for:

Mr. FILNER. Mr. Chair, on rollcall No. 185, I was away from the Capitol due to prior commitments to my constituents. Had I been present, I would have voted ''aye.''

AMENDMENT NO. 6 OFFERED BY MR. QUAYLE

The Acting CHAIR. The unfinished business is the demand for a recorded vote on the amendment offered by the gentleman from Arizona (Mr. QUAYLE) 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 Acting CHAIR. This will be a 2-minute vote.

The vote was taken by electronic device, and there were—ayes 410, noes 3, not voting 18, as follows:

[Roll No. 186]

AYES—410

Ackerman
Adams
Aderholt
Akin
Alexander
Altmire
Amash
Amodei
Andrews
Austria
Baca
Bachmann
Bachus
Baldwin
Barletta
Barrow
Bartlett
Barton (TX)
Bass (CA)
Bass (NH)
Becerra
Benishek
Berg
Berkley
Berman
Biggert
Bilbray
Bilirakis
Bishop (GA)
Bishop (NY)
Bishop (UT)
Black
Blackburn
Bonamici
Bonner
Bono Mack
Boren
Boswell
Boustany
Brady (PA)
Brady (TX)
Braley (IA)
Brooks
Broun (GA)
Brown (FL)
Buchanan
Buerkle
Burgess
Burton (IN)
Butterfield
Calvert
Camp
Campbell
Cantor
Capito
Capps
Capuano
Cardoza
Carnahan
Carney
Carson (IN)
Carter
Cassidy
Castor (FL)
Chabot
Chaffetz
Chandler
Chu
Cicilline
Clarke (MI)
Clarke (NY)
Clay
Cleaver
Clyburn
Coble
Coffman (CO)
Cohen
Cole
Conaway
Connolly (VA)
Conyers
Cooper
Costa
Costello
Courtney
Cravaack
Crawford
Crenshaw
Critz
Crowley
Cuellar
Culberson
Cummings
Davis (CA)
Davis (IL)
DeFazio
DeGette
DeLauro
Denham
Dent
DesJarlais
Deutch
Diaz-Balart
Dicks
Dingell
Doggett
Dold
Donnelly (IN)
Doyle
Dreier
Duffy
Duncan (SC)
Duncan (TN)
Edwards
Ellison
Ellmers
Emerson
Engel
Eshoo
Farenthold
Farr
Fattah
Fincher
Fitzpatrick
Flake
Fleischmann
Fleming
Flores
Forbes
Fortenberry
Foxx
Frank (MA)
Franks (AZ)
Frelinghuysen
Fudge
Gallegly
Garamendi
Gardner
Garrett
Gerlach
Gibbs
Gibson
Gingrey (GA)
Gonzalez
Goodlatte
Gosar
Gowdy
Granger
Graves (GA)
Graves (MO)
Green, Al
Green, Gene
Griffin (AR)
Griffith (VA)
Grijalva
Grimm
Guinta
Guthrie
Gutierrez
Hahn
Hall
Hanabusa
Hanna
Harper
Harris
Hartzler
Hastings (FL)
Hastings (WA)
Hayworth
Heck
Heinrich
Hensarling
Herger
Herrera Beutler
Higgins
Himes
Hinchey
Hinojosa
Hochul
Holt
Honda
Hoyer
Huelskamp
Huizenga (MI)
Hultgren
Hunter
Hurt
Israel
Issa
Jackson (IL)
Jackson Lee (TX)
Jenkins
Johnson (IL)
Johnson (OH)
Johnson, E. B.
Johnson, Sam
Jones
Jordan
Kaptur
Keating
Kelly
Kildee
Kind
King (IA)
King (NY)
Kingston
Kinzinger (IL)
Kissell
Kline
Kucinich
Labrador
Lamborn
Lance
Landry
Langevin
Lankford
Larsen (WA)
Larson (CT)
Latham
LaTourette
Latta

Lee (CA)
Levin
Lewis (CA)
Lewis (GA)
Lipinski
LoBiondo
Loebsack
Long
Lowey
Lucas
Luetkemeyer
Luján
Lummis
Lungren, Daniel E.
Lynch
Mack
Manzullo
Marchant
Markey
Matheson
Matsui
McCarthy (CA)
McCarthy (NY)
McCaul
McCollum
McCotter
McDermott
McGovern
McIntyre
McKeon
McKinley
McMorris Rodgers
McNerney
Meehan
Meeks
Mica
Michaud
Miller (FL)
Miller (MI)
Miller (NC)
Miller, Gary
Miller, George
Moore
Moran
Mulvaney
Murphy (CT)
Murphy (PA)
Myrick
Nadler
Napolitano
Neal
Neugebauer
Noem
Nugent
Nunes
Nunnelee
Olson
Olver
Owens
Palazzo
Pallone
Pascrell
Pastor (AZ)
Paulsen
Pearce
Pelosi
Perlmutter
Peters
Peterson
Petri
Pingree (ME)
Pitts
Platts
Poe (TX)
Polis
Pompeo
Posey
Price (GA)
Price (NC)
Quayle
Quigley
Rahall
Reed
Rehberg
Reichert
Renacci
Reyes
Ribble
Richardson
Richmond
Rigell
Rivera
Roby
Roe (TN)
Rogers (AL)
Rogers (KY)
Rogers (MI)
Rohrabacher
Rokita
Rooney
Ros-Lehtinen
Roskam
Ross (AR)
Ross (FL)
Rothman (NJ)
Roybal-Allard
Royce
Runyan
Ruppersberger
Rush
Ryan (OH)
Ryan (WI)
Sánchez, Linda T.
Sanchez, Loretta
Sarbanes
Scalise
Schakowsky
Schiff
Schilling
Schmidt
Schock
Schwartz
Schweikert
Scott (SC)
Scott (VA)
Scott, Austin
Scott, David
Sensenbrenner
Serrano
Sessions
Sewell
Sherman
Shimkus
Shuler
Shuster
Simpson
Smith (NE)
Smith (NJ)
Smith (TX)
Smith (WA)
Southerland
Speier
Stark
Stearns
Stivers
Stutzman
Sutton
Terry
Thompson (CA)
Thompson (MS)
Thompson (PA)
Thornberry
Tiberi
Tierney
Tipton
Tonko
Towns
Tsongas
Turner (NY)
Turner (OH)
Upton
Van Hollen
Velázquez
Visclosky
Walberg
Walden
Walsh (IL)
Walz (MN)
Wasserman Schultz
Waters
Watt
Waxman
Webster
Welch
West
Westmoreland
Whitfield
Wilson (FL)
Wilson (SC)
Wittman
Wolf
Womack
Woodall
Woolsey
Yarmuth
Yoder
Young (AK)
Young (FL)
Young (IN)

NOES—3

Gohmert
Lofgren, Zoe
McClintock

NOT VOTING—18

Blumenauer
Bucshon
Canseco
Davis (KY)
Filner
Hirono
Holden
Johnson (GA)
Maloney
Marino
McHenry
Paul
Pence
Rangel
Schrader
Sires
Slaughter
Sullivan

□ 1731

So the amendment was agreed to.

The result of the vote was announced as above recorded.

Stated for:

Mr. FILNER. Mr. Chair, on rollcall 186, I was away from the Capitol due to prior commitments to my constituents. Had I been present, I would have voted "aye."

AMENDMENT NO. 7 OFFERED BY AMASH

The Acting CHAIR. The unfinished business is the demand for a recorded vote on the amendment offered by the gentleman from Michigan (Mr. AMASH) 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 Acting CHAIR. This will be a 2-minute vote.

The vote was taken by electronic device, and there were—ayes 415, noes 0, not voting 16, as follows:

[Roll No. 187]

AYES—415

Ackerman
Adams
Aderholt
Akin
Alexander
Altmire
Amash
Amodei
Andrews
Austria
Baca
Bachmann
Bachus
Baldwin
Barletta
Barrow
Bartlett
Barton (TX)
Bass (CA)
Bass (NH)
Becerra
Benishek
Berg
Berkley
Berman
Biggert
Bilbray
Bilirakis
Bishop (GA)
Bishop (NY)
Bishop (UT)
Black
Blackburn
Bonamici
Bonner
Bono Mack
Boren
Boswell
Boustany
Brady (PA)
Brady (TX)
Braley (IA)
Brooks
Broun (GA)
Brown (FL)
Buchanan
Buerkle
Burgess
Burton (IN)
Butterfield
Calvert
Camp
Campbell
Cantor
Capito
Capps
Capuano
Cardoza
Carnahan
Carney
Carson (IN)
Carter
Cassidy
Castor (FL)
Chabot
Chaffetz
Chandler
Chu
Cicilline
Clarke (MI)
Clarke (NY)
Clay
Cleaver
Clyburn
Coble
Coffman (CO)
Cohen
Cole
Conaway
Connolly (VA)
Conyers
Cooper
Costa
Costello
Courtney
Cravaack
Crawford
Crenshaw
Critz
Crowley
Cuellar
Culberson
Cummings
Davis (CA)
Davis (IL)
DeFazio
DeGette
DeLauro
Denham
Dent
DesJarlais
Deutch
Diaz-Balart
Dicks
Dingell
Doggett
Dold
Donnelly (IN)
Doyle
Dreier
Duffy
Duncan (SC)
Duncan (TN)
Edwards
Ellison
Ellmers
Emerson
Engel
Eshoo
Farenthold
Farr
Fattah
Fincher
Fitzpatrick
Flake
Fleischmann
Fleming
Flores
Forbes
Fortenberry
Foxx
Frank (MA)
Franks (AZ)
Frelinghuysen
Fudge
Gallegly
Garamendi
Gardner
Garrett
Gerlach
Gibbs
Gibson
Gingrey (GA)
Gohmert
Gonzalez
Goodlatte
Gosar
Gowdy
Granger
Graves (GA)
Graves (MO)
Green, Al
Green, Gene
Griffin (AR)
Griffith (VA)
Grijalva
Grimm
Guinta
Guthrie
Gutierrez
Hahn
Hall
Hanabusa
Hanna
Harper
Harris
Hartzler
Hastings (FL)
Hastings (WA)
Hayworth
Heck
Heinrich
Hensarling
Herger
Herrera Beutler
Higgins
Himes
Hinchey
Hinojosa
Hochul
Holt
Honda
Hoyer
Huelskamp
Huizenga (MI)
Hultgren
Hunter
Hurt
Israel
Issa
Jackson (IL)
Jackson Lee (TX)
Jenkins
Johnson (IL)
Johnson (OH)
Johnson, E. B.
Johnson, Sam
Jones
Jordan
Kaptur
Keating
Kelly
Kildee
Kind
King (IA)
King (NY)
Kingston
Kinzinger (IL)
Kissell
Kline
Kucinich
Labrador
Lamborn
Lance
Landry
Langevin
Lankford
Larsen (WA)
Larson (CT)
Latham
LaTourette
Latta
Lee (CA)
Levin
Lewis (CA)
Lewis (GA)
Lipinski
LoBiondo
Loebsack
Lofgren, Zoe
Long
Lowey
Lucas
Luetkemeyer
Luján
Lummis
Lungren, Daniel E.
Lynch
Mack
Manzullo
Marchant
Markey
Matheson
Matsui
McCarthy (CA)
McCarthy (NY)
McCaul
McClintock
McCollum
McCotter
McDermott
McGovern
McIntyre
McKeon
McKinley
McMorris Rodgers
McNerney
Meehan
Meeks
Mica
Michaud
Miller (FL)
Miller (MI)
Miller (NC)
Miller, Gary
Miller, George
Moore
Moran
Mulvaney
Murphy (CT)
Murphy (PA)
Myrick
Nadler
Napolitano
Neal
Neugebauer
Noem
Nugent
Nunes
Nunnelee
Olson
Olver
Owens
Palazzo
Pallone
Pascrell
Pastor (AZ)
Paulsen
Pearce
Pelosi
Perlmutter
Peters
Peterson
Petri
Pingree (ME)
Pitts
Platts
Poe (TX)
Polis
Pompeo
Posey
Price (GA)
Price (NC)
Quayle
Quigley
Rahall
Reed
Rehberg
Reichert
Renacci
Reyes
Ribble
Richardson
Richmond
Rigell
Rivera
Roby
Roe (TN)
Rogers (AL)
Rogers (KY)
Rogers (MI)
Rohrabacher
Rokita
Rooney
Ros-Lehtinen
Roskam
Ross (AR)
Ross (FL)
Rothman (NJ)
Roybal-Allard
Royce
Runyan
Ruppersberger
Rush
Ryan (OH)
Ryan (WI)
Sánchez, Linda T.
Sanchez, Loretta
Sarbanes
Scalise
Schakowsky
Schiff
Schilling
Schmidt
Schock
Schrader
Schwartz
Schweikert
Scott (SC)
Scott (VA)
Scott, Austin
Scott, David
Sensenbrenner
Serrano
Sessions
Sewell
Sherman
Shimkus
Shuler
Shuster
Simpson
Smith (NE)
Smith (NJ)
Smith (TX)
Smith (WA)
Southerland
Speier
Stark
Stearns
Stivers
Stutzman
Sullivan
Sutton
Terry
Thompson (CA)
Thompson (MS)
Thompson (PA)
Thornberry
Tiberi
Tierney
Tipton
Tonko
Towns
Tsongas
Turner (NY)
Turner (OH)
Upton
Van Hollen
Velázquez
Visclosky
Walberg
Walden
Walsh (IL)
Walz (MN)
Wasserman Schultz
Waters
Watt
Waxman
Webster
Welch
West
Westmoreland
Whitfield
Wilson (FL)
Wilson (SC)
Wittman
Wolf
Womack
Woodall
Woolsey
Yarmuth
Yoder
Young (AK)
Young (FL)
Young (IN)

NOT VOTING—16

Blumenauer
Bucshon
Canseco
Davis (KY)
Filner
Hirono
Holden
Johnson (GA)
Maloney
Marino
McHenry
Paul
Pence
Rangel
Sires
Slaughter

□ 1736

So the amendment was agreed to.

The result of the vote was announced as above recorded.

Stated for:

Mr. FILNER. Mr. Chair, on rollcall 187, I was away from the Capitol due to prior commitments to my constituents. Had I been present, I would have voted "aye."

AMENDMENT NO. 8 OFFERED BY MR. MULVANEY

The Acting CHAIR. The unfinished business is the demand for a recorded vote on the amendment offered by the gentleman from South Carolina (Mr. MULVANEY) 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 Acting CHAIR. This will be a 2-minute vote.

The vote was taken by electronic device, and there were—ayes 416, noes 0, not voting 15, as follows:

[Roll No. 188]

AYES—416

Ackerman
Adams
Aderholt
Akin
Alexander
Altmire
Amash
Amodei
Andrews
Austria
Baca
Bachmann
Bachus
Baldwin
Barletta
Barrow
Bartlett
Barton (TX)
Bass (CA)
Bass (NH)
Becerra
Benishek
Berg
Berkley
Berman
Biggert
Bilbray
Bilirakis
Bishop (GA)
Bishop (NY)
Bishop (UT)
Black
Blackburn
Bonamici
Bonner
Bono Mack
Boren
Boswell
Boustany
Brady (PA)
Brady (TX)
Braley (IA)
Brooks
Broun (GA)
Brown (FL)
Buchanan
Buerkle
Burgess
Burton (IN)
Butterfield
Calvert
Camp
Campbell
Cantor
Capito
Capps
Capuano
Cardoza
Carnahan
Carney
Carson (IN)
Carter
Cassidy
Castor (FL)
Chabot
Chaffetz
Chandler
Chu
Cicilline
Clarke (MI)
Clarke (NY)
Clay
Cleaver
Clyburn
Coble
Coffman (CO)
Cohen
Cole
Conaway
Connolly (VA)
Conyers
Cooper
Costa
Costello
Courtney
Cravaack
Crawford
Crenshaw
Critz
Crowley
Cuellar
Culberson
Cummings
Davis (CA)
Davis (IL)
DeFazio
DeGette
DeLauro
Denham
Dent
DesJarlais
Deutch
Diaz-Balart
Dicks
Dingell
Doggett
Dold
Donnelly (IN)
Doyle
Dreier
Duffy
Duncan (SC)
Duncan (TN)
Edwards
Ellison
Ellmers
Emerson
Engel
Eshoo
Farenthold
Farr
Fattah
Fincher
Fitzpatrick
Flake
Fleischmann
Fleming
Flores
Forbes
Fortenberry
Foxx
Frank (MA)
Franks (AZ)
Frelinghuysen
Fudge
Gallegly
Garamendi
Gardner
Garrett
Gerlach
Gibbs
Gibson
Gingrey (GA)
Gohmert
Gonzalez
Goodlatte
Gosar
Gowdy
Granger
Graves (GA)
Graves (MO)
Green, Al
Green, Gene
Griffin (AR)
Griffith (VA)
Grijalva
Grimm
Guinta
Guthrie
Gutierrez
Hahn
Hall
Hanabusa
Hanna
Harper
Harris
Hartzler
Hastings (FL)
Hastings (WA)
Hayworth
Heck
Heinrich
Hensarling
Herger
Herrera Beutler
Higgins
Himes
Hinchey
Hinojosa
Hochul
Holt
Honda
Hoyer
Huelskamp
Huizenga (MI)
Hultgren
Hunter
Hurt
Israel
Issa
Jackson (IL)
Jackson Lee (TX)
Jenkins
Johnson (GA)
Johnson (IL)
Johnson (OH)
Johnson, E. B.
Johnson, Sam
Jones
Jordan
Kaptur
Keating
Kelly
Kildee
Kind
King (IA)
King (NY)
Kingston
Kinzinger (IL)
Kissell
Kline
Kucinich
Labrador
Lamborn
Lance
Landry
Langevin
Lankford
Larsen (WA)
Larson (CT)
Latham
LaTourette
Latta
Lee (CA)
Levin
Lewis (CA)
Lewis (GA)
Lipinski
LoBiondo
Loebsack
Lofgren, Zoe
Long
Lowey
Lucas
Luetkemeyer
Luján
Lummis
Lungren, Daniel E.
Lynch
Mack
Manzullo
Marchant
Markey
Matheson
Matsui
McCarthy (CA)
McCarthy (NY)
McCaul
McClintock
McCollum
McCotter
McDermott
McGovern
McIntyre
McKeon
McKinley
McMorris Rodgers
McNerney
Meehan
Meeks
Mica
Michaud
Miller (FL)
Miller (MI)
Miller (NC)
Miller, Gary
Miller, George
Moore
Moran
Mulvaney
Murphy (CT)
Murphy (PA)
Myrick
Nadler
Napolitano
Neal
Neugebauer
Noem
Nugent
Nunes
Nunnelee
Olson
Olver
Owens
Palazzo
Pallone
Pascrell
Pastor (AZ)
Paulsen
Pearce
Pelosi
Perlmutter
Peters
Peterson
Petri
Pingree (ME)
Pitts
Platts
Poe (TX)
Polis
Pompeo
Posey
Price (GA)
Price (NC)
Quayle
Quigley
Rahall
Reed
Rehberg
Reichert
Renacci
Reyes
Ribble
Richardson
Richmond
Rigell
Rivera
Roby
Roe (TN)
Rogers (AL)
Rogers (KY)
Rogers (MI)
Rohrabacher
Rokita
Rooney
Ros-Lehtinen
Roskam
Ross (AR)
Ross (FL)
Rothman (NJ)
Roybal-Allard
Royce
Runyan
Ruppersberger
Rush
Ryan (OH)
Ryan (WI)
Sánchez, Linda T.
Sanchez, Loretta
Sarbanes
Scalise
Schakowsky
Schiff
Schilling
Schmidt
Schock
Schrader
Schwartz
Schweikert
Scott (SC)
Scott (VA)
Scott, Austin
Scott, David
Sensenbrenner
Serrano
Sessions
Sewell
Sherman
Shimkus
Shuler
Shuster
Simpson
Smith (NE)
Smith (NJ)
Smith (TX)
Smith (WA)
Southerland
Speier
Stark
Stearns
Stivers
Stutzman
Sullivan
Sutton
Terry
Thompson (CA)
Thompson (MS)
Thompson (PA)
Thornberry
Tiberi
Tierney
Tipton
Tonko
Towns
Tsongas
Turner (NY)
Turner (OH)
Upton
Van Hollen
Velázquez
Visclosky
Walberg
Walden
Walsh (IL)
Walz (MN)
Wasserman Schultz
Waters
Watt
Waxman
Webster
Welch
West
Westmoreland
Whitfield
Wilson (FL)
Wilson (SC)
Wittman
Wolf
Womack
Woodall
Woolsey
Yarmuth
Yoder
Young (AK)
Young (FL)
Young (IN)

NOT VOTING—15

Blumenauer
Bucshon
Canseco
Davis (KY)
Filner
Hirono
Holden
Maloney
Marino
McHenry
Paul
Pence
Rangel
Sires
Slaughter

□ 1740

So the amendment was agreed to.

The result of the vote was announced as above recorded.

Stated for:

Mr. FILNER. Mr. Chair, on rollcall 188, I was away from the Capitol due to prior commitments to my constituents. Had I been present, I would have voted "aye."

AMENDMENT NO. 13 OFFERED BY MR. GOODLATTE

The Acting CHAIR. The unfinished business is the demand for a recorded vote on the amendment offered by the gentleman from Virginia (Mr. GOODLATTE) 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 Acting CHAIR. This will be a 2-minute vote.

The vote was taken by electronic device, and there were—ayes 414, noes 1, not voting 16, as follows:

[Roll No. 189]

AYES—414

Ackerman
Adams
Aderholt
Alexander
Altmire
Amash
Amodei
Andrews
Austria
Baca
Bachmann
Bachus
Baldwin
Barletta
Barrow
Bartlett
Barton (TX)
Bass (CA)
Bass (NH)
Becerra
Benishek
Berg
Berkley
Berman
Biggert
Bilbray
Bilirakis
Bishop (GA)
Bishop (NY)
Bishop (UT)
Black
Blackburn
Bonamici
Bonner
Bono Mack
Boren
Boswell
Boustany
Brady (PA)
Brady (TX)
Braley (IA)
Brooks
Broun (GA)
Brown (FL)
Buchanan
Buerkle
Burgess
Burton (IN)
Butterfield
Calvert
Camp
Campbell
Cantor
Capito
Capps
Capuano
Cardoza
Carnahan
Carney
Carson (IN)
Carter
Cassidy
Castor (FL)
Chabot
Chaffetz
Chandler
Chu
Cicilline
Clarke (MI)
Clarke (NY)
Clay
Cleaver
Clyburn
Coble
Coffman (CO)
Cohen
Cole
Conaway
Connolly (VA)
Conyers
Cooper
Costa
Costello
Courtney
Cravaack
Crawford
Crenshaw
Critz
Crowley
Cuellar
Culberson
Cummings
Davis (CA)
Davis (IL)
DeFazio
DeGette
DeLauro
Denham
Dent
DesJarlais
Deutch
Diaz-Balart
Dicks
Dingell
Doggett
Dold
Donnelly (IN)
Doyle
Dreier
Duffy
Duncan (SC)
Duncan (TN)
Edwards
Ellison
Ellmers
Emerson
Engel
Eshoo
Farenthold
Farr
Fattah
Fincher
Fitzpatrick
Flake
Fleischmann
Fleming
Flores
Forbes
Fortenberry
Foxx
Frank (MA)
Franks (AZ)
Frelinghuysen
Fudge
Gallegly
Garamendi
Gardner
Garrett
Gerlach
Gibbs
Gibson
Gingrey (GA)
Gohmert
Gonzalez
Goodlatte
Gosar
Gowdy
Granger
Graves (GA)
Graves (MO)
Green, Al
Green, Gene
Griffin (AR)
Griffith (VA)
Grijalva
Grimm
Guinta
Guthrie
Gutierrez
Hahn
Hall
Hanabusa
Hanna
Harper
Harris
Hartzler
Hastings (FL)
Hastings (WA)
Hayworth
Heck
Heinrich
Hensarling
Herger
Herrera Beutler
Higgins
Himes
Hinchey
Hinojosa
Hochul
Holt
Honda
Hoyer
Huelskamp
Huizenga (MI)
Hultgren
Hunter
Hurt
Israel
Issa
Jackson (IL)
Jackson Lee (TX)
Jenkins
Johnson (GA)
Johnson (IL)
Johnson (OH)
Johnson, E. B.
Johnson, Sam
Jones
Jordan
Kaptur
Keating
Kelly
Kildee
Kind
King (IA)
King (NY)
Kingston
Kinzinger (IL)
Kissell
Kline
Kucinich
Labrador
Lamborn
Lance
Landry
Langevin
Lankford
Larsen (WA)
Larson (CT)
Latham
LaTourette
Latta
Lee (CA)
Levin
Lewis (CA)
Lewis (GA)
Lipinski
LoBiondo
Loebsack
Long
Lowey
Lucas
Luetkemeyer
Luján
Lummis
Lungren, Daniel E.
Lynch
Mack
Manzullo
Marchant
Markey
Matheson
Matsui
McCarthy (CA)
McCarthy (NY)
McCaul
McClintock
McCollum
McCotter
McDermott
McGovern
McIntyre
McKeon
McKinley
McMorris Rodgers
McNerney
Meehan
Meeks
Mica
Michaud
Miller (FL)
Miller (MI)
Miller (NC)
Miller, Gary
Miller, George
Moore
Moran
Mulvaney
Murphy (CT)
Murphy (PA)
Myrick
Nadler
Napolitano

Neal
Neugebauer
Noem
Nugent
Nunes
Nunnelee
Olson
Olver
Owens
Palazzo
Pallone
Pascrell
Pastor (AZ)
Paulsen
Pearce
Pelosi
Perlmutter
Peters
Peterson
Petri
Pingree (ME)
Pitts
Platts
Poe (TX)
Polis
Pompeo
Posey
Price (GA)
Price (NC)
Quayle
Quigley
Rahall
Reed
Rehberg
Reichert
Renacci
Reyes
Ribble
Richardson
Richmond
Rigell
Rivera
Roby
Roe (TN)
Rogers (AL)
Rogers (KY)
Rogers (MI)
Rohrabacher
Rokita
Rooney
Ros-Lehtinen
Roskam
Ross (AR)
Ross (FL)
Rothman (NJ)
Roybal-Allard
Royce
Runyan
Ruppersberger
Rush
Ryan (OH)
Ryan (WI)
Sánchez, Linda T.
Sanchez, Loretta
Sarbanes
Scalise
Schakowsky
Schiff
Schilling
Schmidt
Schock
Schrader
Schwartz
Schweikert
Scott (SC)
Scott (VA)
Scott, Austin
Scott, David
Sensenbrenner
Serrano
Sessions
Sewell
Sherman
Shimkus
Shuler
Shuster
Simpson
Smith (NE)
Smith (NJ)
Smith (TX)
Smith (WA)
Southerland
Speier
Stark
Stearns
Stivers
Stutzman
Sullivan
Sutton
Terry
Thompson (CA)
Thompson (MS)
Thompson (PA)
Thornberry
Tiberi
Tierney
Tipton
Tonko
Towns
Tsongas
Turner (NY)
Turner (OH)
Upton
Van Hollen
Velázquez
Visclosky
Walberg
Walden
Walsh (IL)
Walz (MN)
Wasserman Schultz
Waters
Watt
Waxman
Webster
Welch
West
Westmoreland
Whitfield
Wilson (FL)
Wilson (SC)
Wittman
Wolf
Womack
Woodall
Woolsey
Yarmuth
Yoder
Young (AK)
Young (FL)
Young (IN)

NOES—1

Lofgren, Zoe

NOT VOTING—16

Akin
Blumenauer
Bucshon
Canseco
Davis (KY)
Filner
Hirono
Holden
Maloney
Marino
McHenry
Paul
Pence
Rangel
Sires
Slaughter

□ 1744

So the amendment was agreed to.

The result of the vote was announced as above recorded.

Stated for:

Mr. FILNER. Mr. Chair, on rollcall 189, I was away from the Capitol due to prior commitments to my constituents. Had I been present, I would have voted "aye."

AMENDMENT NO. 15 OFFERED BY MR. MULVANEY

The Acting CHAIR. The unfinished business is the demand for a recorded vote on the amendment offered by the gentleman from South Carolina (Mr. MULVANEY) 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 Acting CHAIR. This will be a 2-minute vote.

The vote was taken by electronic device, and there were—ayes 413, noes 3, not voting 15, as follows:

[Roll No. 190]

AYES—413

Ackerman
Adams
Aderholt
Akin
Alexander
Altmire
Amash
Amodei
Andrews
Austria
Baca
Bachmann
Bachus
Baldwin
Barletta
Barrow
Bartlett
Barton (TX)
Bass (CA)
Bass (NH)
Becerra
Benishek
Berg
Berkley
Berman
Biggert
Bilbray
Bilirakis
Bishop (GA)
Bishop (NY)
Bishop (UT)
Black
Blackburn
Bonamici
Bonner
Bono Mack
Boren
Boswell
Boustany
Brady (PA)
Brady (TX)
Braley (IA)
Brooks
Broun (GA)
Brown (FL)
Buchanan
Buerkle
Burgess
Burton (IN)
Butterfield
Calvert
Camp
Campbell
Cantor
Capito
Capps
Capuano
Cardoza
Carnahan
Carney
Carson (IN)
Carter
Cassidy
Castor (FL)
Chabot
Chaffetz
Chandler
Chu
Cicilline
Clarke (MI)
Clarke (NY)
Clay
Cleaver
Clyburn
Coble
Coffman (CO)
Cohen
Cole
Conaway
Connolly (VA)
Conyers
Cooper
Costa
Costello
Courtney
Cravaack
Crawford
Crenshaw
Critz
Crowley
Cuellar
Culberson
Cummings
Davis (CA)
Davis (IL)
DeFazio
DeGette
DeLauro
Denham
Dent
DesJarlais
Deutch
Diaz-Balart
Dicks
Doggett
Dold
Donnelly (IN)
Doyle
Dreier
Duffy
Duncan (SC)
Duncan (TN)
Edwards
Ellison
Ellmers
Emerson
Engel
Eshoo
Farenthold
Farr
Fattah
Fincher
Fitzpatrick
Flake
Fleischmann
Fleming
Flores
Forbes
Fortenberry
Foxx
Frank (MA)
Franks (AZ)
Frelinghuysen
Fudge
Gallegly
Garamendi
Gardner
Garrett
Gerlach
Gibbs
Gibson
Gingrey (GA)
Gohmert
Gonzalez
Goodlatte
Gosar
Gowdy
Granger
Graves (GA)
Graves (MO)
Green, Al
Green, Gene
Griffin (AR)
Griffith (VA)
Grijalva
Grimm
Guinta
Guthrie
Gutierrez
Hahn
Hall
Hanabusa
Hanna
Harper
Harris
Hartzler
Hastings (FL)
Hastings (WA)
Hayworth
Heck
Heinrich
Hensarling
Herger
Herrera Beutler
Higgins
Himes
Hinchey
Hinojosa
Hochul
Holt
Honda
Hoyer
Huelskamp
Huizenga (MI)
Hultgren
Hunter
Hurt
Israel
Issa
Jackson (IL)
Jackson Lee (TX)
Jenkins
Johnson (GA)
Johnson (IL)
Johnson (OH)
Johnson, E. B.
Johnson, Sam
Jones
Jordan
Kaptur
Keating
Kelly
Kildee
Kind
King (IA)
King (NY)
Kingston
Kinzinger (IL)
Kissell
Kline
Kucinich
Labrador
Lamborn
Lance
Landry
Langevin
Lankford
Larsen (WA)
Larson (CT)
Latham
LaTourette
Latta
Lee (CA)
Levin
Lewis (CA)
Lewis (GA)
Lipinski
LoBiondo
Loebsack
Lofgren, Zoe
Long
Lowey
Lucas
Luetkemeyer
Luján
Lummis
Lungren, Daniel E.
Lynch
Mack
Manzullo
Marchant
Markey
Matheson
Matsui
McCarthy (CA)
McCarthy (NY)
McCaul
McClintock
McCollum
McCotter
McDermott
McGovern
McIntyre
McKeon
McKinley
McMorris Rodgers
McNerney
Meehan
Meeks
Mica
Michaud
Miller (FL)
Miller (MI)
Miller (NC)
Miller, Gary
Miller, George
Moore
Moran
Mulvaney
Murphy (CT)
Murphy (PA)
Myrick
Nadler
Napolitano
Neal
Neugebauer
Noem
Nugent
Nunes
Nunnelee
Olson
Olver
Owens
Palazzo
Pallone
Pascrell
Pastor (AZ)
Paulsen
Pearce
Pelosi
Perlmutter
Peters
Peterson
Petri
Pingree (ME)
Pitts
Platts
Poe (TX)
Polis
Pompeo
Posey
Price (GA)
Price (NC)
Quayle
Quigley
Rahall
Reed
Rehberg
Reichert
Renacci
Reyes
Ribble
Richardson
Richmond
Rigell
Rivera
Roby
Roe (TN)
Rogers (AL)
Rogers (KY)
Rogers (MI)
Rohrabacher
Rokita
Rooney
Ros-Lehtinen
Roskam
Ross (AR)
Ross (FL)
Rothman (NJ)
Roybal-Allard
Royce
Runyan
Ruppersberger
Rush
Ryan (OH)
Ryan (WI)
Sánchez, Linda T.
Sanchez, Loretta
Sarbanes
Scalise
Schakowsky
Schiff
Schilling
Schmidt
Schock
Schwartz
Schweikert
Scott (SC)
Scott (VA)
Scott, Austin
Scott, David
Sensenbrenner
Serrano
Sessions
Sewell
Sherman
Shimkus
Shuler
Shuster
Simpson
Smith (NE)
Smith (NJ)
Smith (TX)
Smith (WA)
Southerland
Speier
Stark
Stearns
Stivers
Stutzman
Sullivan
Sutton
Terry
Thompson (CA)
Thompson (MS)
Thompson (PA)
Thornberry
Tiberi
Tierney
Tipton
Tonko
Towns
Tsongas
Turner (OH)
Upton
Van Hollen
Velázquez
Visclosky
Walberg
Walden
Walsh (IL)
Walz (MN)
Wasserman Schultz
Waters
Watt
Waxman
Webster
Welch
West
Westmoreland
Whitfield
Wilson (FL)
Wilson (SC)
Wittman
Wolf
Womack
Woodall
Woolsey
Yarmuth
Yoder
Young (AK)
Young (FL)
Young (IN)

NOES—3

Dingell
Schrader
Turner (NY)

NOT VOTING—15

Blumenauer
Bucshon
Canseco
Davis (KY)
Filner
Hirono
Holden
Maloney
Marino
McHenry
Paul
Pence
Rangel
Sires
Slaughter

□ 1747

So the amendment was agreed to.

The result of the vote was announced as above recorded.

Stated for:

Mr. FILNER. Mr. Chair, on rollcall 190, I was away from the Capitol due to prior commitments to my constituents. Had I been present, I would have voted "aye."

The Acting CHAIR. The question is on the amendment in the nature of a substitute, as amended.

The amendment was agreed to.

The Acting CHAIR. Under the rule, the Committee rises.

Accordingly, the Committee rose; and the Speaker pro tempore (Mr. WOODALL) having assumed the chair, Mr. CHAFFETZ, Acting Chair of the Committee of the Whole House on the state of the Union, reported that that Committee, having had under consideration the bill (H.R. 3523) 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, and, pursuant to House Resolution 631, he reported the bill back to the House with an amendment adopted in the Committee of the Whole.

The SPEAKER pro tempore. Under the rule, the previous question is ordered.

Is a separate vote demanded on any amendment to the amendment reported from the Committee of the Whole?

If not, the question is on the amendment in the nature of a substitute, as amended.

The amendment was agreed to.

The SPEAKER pro tempore. The question is on the engrossment and third reading of the bill.

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

MOTION TO RECOMMIT

Mr. PERLMUTTER. Mr. Speaker, I have a motion to recommit at the desk.

The SPEAKER pro tempore. Is the gentleman opposed to the bill?

Mr. PERLMUTTER. In its current form, I am.

The SPEAKER pro tempore. The Clerk will report the motion to recommit.

The Clerk read as follows:

Mr. Perlmutter moves to recommit the bill, H.R. 3523, to the Permanent Select Committee on Intelligence with instructions to report the same back to the House forthwith with the following amendments:

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

SEC. 3. PROTECTING THE PRIVACY OF INTERNET PASSWORDS AND THE CREATIVITY OF THE INTERNET.

Nothing in this Act or the amendments made by this Act shall be construed to—

(1) permit an employer, a prospective employer, or the Federal Government to require the disclosure of a confidential password for a social networking website or a personal account of an employee or job applicant without a court order; or

(2) permit the Federal Government to establish a mechanism to control United States citizens' access to and use of the Internet through the creation of a national Internet firewall similar to the ''Great Internet Firewall of China'', as determined by the Director of the National Intelligence.

Page 12, line 22, strike ''and''.

Page 12, line 25, strike the period and insert a semicolon.

Page 12, after line 25, insert the following:

''(G) the number of Americans who have—

''(i) been required by employers, prospective employers, or the Federal Government to release confidential passwords for social networking websites; and

''(ii) had personal information released to the Federal Government under this section or obtained in connection with a cybersecurity breach; and

''(H) the impact of the information that has been released or obtained as referred to in subparagraph (G) on privacy, electronic commerce, Internet usage, and online content.

The SPEAKER pro tempore. The gentleman from Colorado is recognized for 5 minutes.

Mr. PERLMUTTER. Mr. Speaker, the House has heard this before. It's very simple, sweet and direct, and I will take a moment and just read it so that everybody has a chance to understand it again. What we're doing is avoiding and prohibiting an employer, as a condition of employment, from demanding a confidential Facebook password—Twitter, Tumblr—or any social media of the like. It reads this way:

Nothing in this act or the amendments made by this act shall be construed to permit an employer, a prospective employer, or the Federal Government to require the disclosure of a confidential password for a social networking Web site or a personal account of an employee or job applicant without a court order; or permit the Federal Government to establish a mechanism to control United States citizens' access to and use of the Internet through the creation of a national Internet firewall, similar to the ''Great Internet Firewall of China'', as determined by the Director of National Intelligence.

So what this amendment does is two things. It is the final amendment to this bill. There are no more amendments to this bill. I know some people voted against this amendment when it was brought up a couple of weeks ago; and for those of you who regret voting against it, you're going to get a chance to correct that vote. This is something I've been working on with Mr. HEINRICH and Mr. MCHENRY. It just says we're not going to allow as a condition of employment the requirement of a Facebook password or the like. Now, there is a reason for this.

One, there is all sorts of personal information that I may have or that somebody else may have with respect to Facebook or Twitter or LinkedIn, whatever it might be; and they're entitled to have an expectation of privacy, a sense that their freedom of speech—their freedom to peaceably assemble, in effect—is not violated. So that's the first reason.

The second reason is if an employer or the Federal Government poses as somebody, by having their Facebook passwords, then they can impersonate; they can become imposters. It is a two-way exchange of information so that somebody who is completely unrelated to the employment now is communicating with an impostor. That's another reason for this.

The third reason is for the employers, themselves, to avoid liability by learning information that may then cause them to take actions that would violate a protected group. So there are at least three good reasons to do this.

We have precedent in our law, and it is the Employee Polygraph Protection Act of 1988. We said we're not going to allow as a condition of employment the use of lie detectors. You can use background checks, and you can use references. There are plenty of vehicles by which to check out somebody's employment references; but we're not going to allow lie detectors, and we should not allow that the Facebook passwords be given up as a condition of employment. So we have precedent in the law. We don't allow polygraphs or lie detectors as a condition of employment. Let's use what we already have—background checks, references, et cetera.

The second piece of this is that we will not allow the command and control of the Internet or access to the Internet by the United States Government, saying that which is similar: that we want to avoid what has happened in China, that we want to avoid what has happened in Iran. We don't want the Internet taken down and our access, individuals' access, to the Internet broken.

So there are two pieces to this. One is not allowing the demand of a confidential password and not allowing the government to have the command and control and the ability to take down the Internet, an action similar to what we've seen in other countries.

This is a very simple amendment. It's very straightforward. We've had a lot of amendments that have garnered the support of virtually every Member of this House. This should be one of those. This is the final amendment. I would hope that we would uphold the Constitution by passing this amendment, as well as by making sure that the Internet is available to anyone who wants to use it at any time.

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

Mr. ROGERS of Michigan. I rise in opposition to the motion to recommit.

The SPEAKER pro tempore. The gentleman is recognized for 5 minutes.

Mr. ROGERS of Michigan. Today, 300,000 times somebody will be trying to get into our credit card companies—300,000 times, one company. In just the last few years, just in defense contractors, foreign nation-states have stolen more intellectual property, which will end up protecting this country, equivalent to 50 times the print collection of our U.S. Library of Congress. Anonymous is attacking businesses, and today attacked Wall Street because they're anti-capitalists. There are people out there today who are literally robbing the future of America for our jobs, our prosperity, and our economic prowess in the world; and they're doing it by design.

A year ago, we set out to try to do something small. If we have some bad software—some bad, malicious virus information—shouldn't we be obligated to share that with the private sector so they can protect themselves? Absolutely.

If we don't do this, a nation-state like China has geared up its military and intelligence services for the very purpose of economically wounding the United States—by draining our intellectual property dry. They have done it by stealing pesticide formulas. They have done it by stealing pharmaceutical formulas. They have done it by stealing intellectual property when it relates to military hardware and then have copied it, and it has cost us a tremendous amount of more money to have had to go back and redesign it.

□ 1800

So we can play games. We can do silly things. This amendment actually does nothing to protect a person's private password at home. Nothing. Not one thing. But it is serving to try to obfuscate and maybe send it back to committee and come back.

This has been a bipartisan bill, and I can't tell you how disappointing this amendment is to me. I have worked with Mr. RUPPERSBERGER and the members of this committee. I have worked with the privacy groups. We've worked with civil libertarians. They threw everything but the kitchen sink at us. By the way, this does nothing, or this would have been thrown at us, too. You know why? Because it doesn't do anything. I get it. Sounds great. You're going to run out and do some bad things with it.

But this is our Nation's defense. This is the last bastion of things we need to do to protect this country. We've done it since 9/11. We did Homeland Security. We've done the Patriot Act. We've done other things that this body and the other body and the President of the United States signed to protect this country, as our Constitution tells us to do for the common defense of this great Nation.

I will tell you something. We can have this debate. We can talk about a bill that does absolutely nothing to protect someone's private password at home, or we can get about the business of trying to give the private sector just a little bit of information to protect people's private information in the comfort of their homes, so that we can protect this Nation from a catastrophic attack.

The director of the national security didn't say ''maybe,'' didn't say, ''could happen.'' They said it will happen.

This is the one small thing we get to do to prepare for a whole bunch of folks out there that want to bring this Nation down.

We ought to stand together today in a bipartisan way. We ought to reject all of the confusion and obfuscation and all of the things that they're saying about this bill that just are not true. We ought to stand here and say, We respected the fact that you kept the government stuff government, and the private stuff private, and you're not mixing it up, and you're not surveilling. You're doing none of those things. You're just sharing some pretty bad information so that they can apply it to their patches that happen on your computer every single day, thousands of times a day, to try to keep viruses off your computer, and that's it.

We've spent a lot of time today trying to go in a different direction. People are upset that there aren't things in the bill. Okay. I mean, the Buffett rule isn't in the bill. I don't think that ought to get a veto threat either.

This is where we are. This is that first small threat.

I'm going to ask all of you to join us today. Reject this red herring, this obfuscation, and stand with America. They need it. There are 3 million businesses with all of the associations telling us, Please, give us that classified secret malware information that your government has so we can protect the people we have as customers and clients. They're begging for it because they're getting killed every single day. It's happening right this second.

This is our chance to stand up. This was a bipartisan effort. If you really believe in bipartisanship, if you believe that's the future of this Chamber, and that's the dignity of the very Founding Fathers that gave it to us, then today is the day to prove it.

Reject this amendment, stand for America. Support this bill.

I yield back the balance of my time.

The SPEAKER pro tempore. Without objection, the previous question is ordered on the motion to recommit.

There was no objection.

The SPEAKER pro tempore. The question is on the motion to recommit.

The question was taken; and the Speaker pro tempore announced that the noes appeared to have it.

Mr. PERLMUTTER. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clauses 8 and 9 of rule XX, this 15-minute vote on the motion to recommit will be followed by 5-minute votes on passage of H.R. 3523, if ordered; and suspension of the rules with regard to H.R. 2050, if ordered.

The vote was taken by electronic device, and there were—yeas 183, nays 233, not voting 15, as follows:

[Roll No. 191]

YEAS—183

Ackerman
Altmire
Andrews
Baca
Baldwin
Barrow
Bass (CA)
Becerra
Berkley
Berman
Bishop (GA)
Bishop (NY)
Bonamici
Boren
Boswell
Brady (PA)
Braley (IA)
Brown (FL)
Butterfield
Capps
Capuano
Cardoza
Carnahan
Carney
Carson (IN)
Castor (FL)
Chandler
Chu
Cicilline
Clarke (MI)
Clarke (NY)
Clay
Cleaver
Clyburn
Cohen
Connolly (VA)
Conyers
Cooper
Costa
Costello
Courtney
Critz
Crowley
Cuellar
Cummings
Davis (CA)
Davis (IL)
DeFazio
DeGette
DeLauro
Deutch
Dicks
Dingell
Doggett
Donnelly (IN)
Doyle
Edwards
Ellison
Engel
Eshoo
Farr
Fattah
Frank (MA)
Fudge
Garamendi
Gonzalez
Green, Al
Green, Gene
Grijalva
Gutierrez
Hahn
Hanabusa
Hastings (FL)
Heinrich
Higgins
Himes
Hinchey
Hinojosa
Hochul
Holt
Honda
Hoyer
Israel
Jackson (IL)
Jackson Lee (TX)
Johnson (GA)
Johnson, E. B.
Jones
Kaptur
Keating
Kildee
Kind
Kissell
Kucinich
Langevin
Larsen (WA)
Larson (CT)
Lee (CA)
Levin
Lewis (GA)
Lipinski
Loebsack
Lofgren, Zoe
Lowey
Luján
Lynch
Markey
Matheson
Matsui
McCarthy (NY)
McCollum
McDermott
McGovern
McIntyre
McNerney
Meeks
Michaud
Miller (NC)
Miller, George
Moore
Moran
Murphy (CT)
Nadler
Napolitano
Neal
Olver
Owens
Pallone
Pascrell
Pastor (AZ)
Pelosi
Perlmutter
Peters
Peterson
Pingree (ME)
Polis
Price (NC)
Quigley
Rahall
Reyes
Richardson
Richmond
Ross (AR)
Rothman (NJ)
Roybal-Allard
Ruppersberger
Rush
Ryan (OH)
Sánchez, Linda T.
Sanchez, Loretta
Sarbanes
Schakowsky
Schiff
Schrader
Schwartz
Scott (VA)
Scott, David
Serrano
Sewell
Sherman
Shuler
Smith (WA)
Speier
Stark
Sutton
Thompson (CA)
Thompson (MS)
Tierney
Tonko
Towns
Tsongas
Van Hollen
Velázquez
Visclosky
Walz (MN)
Wasserman Schultz
Waters
Watt
Waxman
Welch
Wilson (FL)
Woolsey
Yarmuth

NAYS—233

Adams
Aderholt
Akin
Alexander
Amash
Amodei
Austria
Bachmann
Bachus
Barletta
Bartlett
Barton (TX)
Bass (NH)
Benishek
Berg
Biggert
Bilbray
Bilirakis
Bishop (UT)
Black
Blackburn
Bonner
Bono Mack
Boustany
Brady (TX)
Brooks
Broun (GA)
Buchanan
Buerkle
Burgess
Burton (IN)
Calvert
Camp
Campbell
Cantor
Capito
Carter
Cassidy
Chabot
Chaffetz
Coble
Coffman (CO)
Cole
Conaway
Cravaack
Crawford
Crenshaw
Culberson
Denham
Dent
DesJarlais
Diaz-Balart
Dold
Dreier
Duffy
Duncan (SC)
Duncan (TN)
Ellmers
Emerson
Farenthold
Fincher
Fitzpatrick
Flake
Fleischmann
Fleming
Flores
Forbes
Fortenberry
Foxx
Franks (AZ)
Frelinghuysen
Gallegly
Gardner
Garrett
Gerlach
Gibbs
Gibson
Gingrey (GA)
Gohmert
Goodlatte
Gosar
Gowdy
Granger
Graves (GA)
Graves (MO)
Griffin (AR)
Griffith (VA)
Grimm
Guinta
Guthrie
Hall
Hanna
Harper
Harris
Hartzler
Hastings (WA)
Hayworth
Heck
Hensarling
Herger
Herrera Beutler
Huelskamp
Huizenga (MI)
Hultgren
Hunter
Hurt
Issa
Jenkins
Johnson (IL)
Johnson (OH)
Johnson, Sam
Jordan
Kelly
King (IA)
King (NY)
Kingston
Kinzinger (IL)
Kline
Labrador
Lamborn
Lance
Landry
Lankford
Latham
LaTourette
Latta
Lewis (CA)
LoBiondo
Long
Lucas
Luetkemeyer
Lummis
Lungren, Daniel E.
Mack
Manzullo
Marchant
McCarthy (CA)
McCaul
McClintock
McCotter
McKeon
McKinley
McMorris Rodgers
Meehan
Mica
Miller (FL)
Miller (MI)
Miller, Gary
Mulvaney
Murphy (PA)
Myrick
Neugebauer
Noem
Nugent
Nunes
Nunnelee
Olson
Palazzo
Paulsen
Pearce
Petri
Pitts
Platts
Poe (TX)
Pompeo
Posey
Price (GA)
Quayle
Reed
Rehberg
Reichert
Renacci
Ribble
Rigell
Rivera
Roby
Roe (TN)
Rogers (AL)
Rogers (KY)
Rogers (MI)
Rohrabacher
Rokita
Rooney
Ros-Lehtinen
Roskam
Ross (FL)
Royce
Runyan
Ryan (WI)
Scalise
Schilling
Schmidt
Schock
Schweikert
Scott (SC)
Scott, Austin
Sensenbrenner
Sessions
Shimkus
Shuster
Simpson
Smith (NE)
Smith (NJ)
Smith (TX)
Southerland
Stearns
Stivers
Stutzman
Sullivan
Terry
Thompson (PA)
Thornberry
Tiberi
Tipton
Turner (NY)
Turner (OH)
Upton
Walberg
Walden
Walsh (IL)
Webster
West
Westmoreland
Whitfield
Wilson (SC)
Wittman
Wolf
Womack
Woodall
Yoder
Young (AK)
Young (FL)
Young (IN)

NOT VOTING—15

Blumenauer
Bucshon
Canseco
Davis (KY)
Filner
Hirono
Holden
Maloney
Marino
McHenry
Paul
Pence
Rangel
Sires
Slaughter

□ 1823

So the motion to recommit was rejected.

The result of the vote was announced as above recorded.

Stated for:

Mr. FILNER. Mr. Speaker, on rollcall 191, I was away from the Capitol due to prior commitments to my constituents. Had I been present, I would have voted "aye."

The SPEAKER pro tempore. The question is on the passage of the bill.

The question was taken; and the Speaker pro tempore announced that the noes appeared to have it.

RECORDED VOTE

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

A recorded vote was ordered.

The SPEAKER pro tempore. This will be a 5-minute vote.

The vote was taken by electronic device, and there were—ayes 248, noes 168, not voting 15, as follows:

[Roll No. 192]

AYES—248

Adams	Dicks	Kissell
Aderholt	Dold	Kline
Alexander	Donnelly (IN)	Labrador
Altmire	Dreier	Lamborn
Amodei	Duffy	Lance
Austria	Duncan (SC)	Langevin
Bachmann	Duncan (TN)	Lankford
Bachus	Ellmers	Larsen (WA)
Barletta	Fincher	Latham
Barrow	Fitzpatrick	LaTourette
Bartlett	Flake	Latta
Bass (NH)	Fleischmann	Lewis (CA)
Benishek	Flores	Lipinski
Berg	Forbes	LoBiondo
Biggert	Fortenberry	Long
Bilbray	Foxx	Lucas
Bilirakis	Franks (AZ)	Luetkemeyer
Bishop (GA)	Frelinghuysen	Lummis
Bishop (NY)	Gallegly	Lungren, Daniel E.
Black	Garamendi	
Blackburn	Gardner	Manzullo
Bonner	Garrett	Matheson
Bono Mack	Gerlach	McCarthy (CA)
Boren	Gibbs	McCarthy (NY)
Boswell	Gingrey (GA)	McCaul
Boustany	Gonzalez	McIntyre
Brady (TX)	Goodlatte	McKeon
Broun (GA)	Gowdy	McKinley
Buchanan	Granger	McMorris Rodgers
Buerkle	Graves (GA)	
Burgess	Graves (MO)	Meehan
Burton (IN)	Griffin (AR)	Mica
Butterfield	Griffith (VA)	Miller (FL)
Calvert	Grimm	Miller (MI)
Camp	Guinta	Miller, Gary
Campbell	Guthrie	Moran
Cantor	Hanabusa	Mulvaney
Capito	Hanna	Murphy (PA)
Cardoza	Harper	Myrick
Carney	Harris	Neugebauer
Carter	Hartzler	Noem
Cassidy	Hastings (WA)	Nugent
Castor (FL)	Hayworth	Nunes
Chabot	Heck	Nunnelee
Chaffetz	Hensarling	Olson
Chandler	Herger	Owens
Clyburn	Herrera Beutler	Palazzo
Coble	Hochul	Paulsen
Coffman (CO)	Huelskamp	Peterson
Cole	Huizenga (MI)	Petri
Conaway	Hultgren	Pitts
Connolly (VA)	Hunter	Platts
Cooper	Hurt	Poe (TX)
Costa	Israel	Pompeo
Cravaack	Issa	Price (GA)
Crawford	Jenkins	Quayle
Crenshaw	Johnson (OH)	Reed
Critz	Johnson, Sam	Reichert
Cuellar	Jordan	Renacci
Culberson	Kelly	Ribble
Denham	King (IA)	Rivera
Dent	King (NY)	Roby
DesJarlais	Kingston	Roe (TN)
Diaz-Balart	Kinzinger (IL)	Rogers (AL)
Rogers (KY)	Sessions	Turner (NY)
Rogers (MI)	Shimkus	Turner (OH)
Rokita	Shuler	Upton
Rooney	Shuster	Walberg
Ros-Lehtinen	Smith (NE)	Walden
Roskam	Smith (NJ)	Webster
Ross (AR)	Smith (TX)	West
Ross (FL)	Smith (WA)	Westmoreland
Royce	Southerland	Whitfield
Runyan	Stearns	Wilson (SC)
Ruppersberger	Stivers	Wittman
Ryan (WI)	Stutzman	Wolf
Scalise	Sullivan	Womack
Schilling	Terry	Woodall
Schmidt	Thompson (CA)	Yoder
Schock	Thompson (PA)	Young (AK)
Schrader	Thornberry	Young (FL)
Scott (SC)	Tiberi	Young (IN)
Scott, Austin	Tipton	
Scott, David	Towns	

NOES—168

Ackerman	Green, Gene	Pascrell
Akin	Grijalva	Pastor (AZ)
Amash	Gutierrez	Pearce
Andrews	Hahn	Pelosi
Baca	Hall	Perlmutter
Baldwin	Hastings (FL)	Peters
Barton (TX)	Heinrich	Pingree (ME)
Bass (CA)	Higgins	Polis
Becerra	Himes	Posey
Berkley	Hinchey	Price (NC)
Berman	Hinojosa	Quigley
Bishop (UT)	Holt	Rahall
Bonamici	Honda	Rehberg
Brady (PA)	Hoyer	Reyes
Braley (IA)	Jackson (IL)	Richardson
Brooks	Jackson Lee (TX)	Richmond
Brown (FL)		Rigell
Capps	Johnson (GA)	Rohrabacher
Capuano	Johnson (IL)	Rothman (NJ)
Carnahan	Johnson, E. B.	Roybal-Allard
Carson (IN)	Jones	Rush
Chu	Kaptur	Ryan (OH)
Cicilline	Keating	Sánchez, Linda T.
Clarke (MI)	Kildee	
Clarke (NY)	Kind	Sanchez, Loretta
Clay	Kucinich	Sarbanes
Cleaver	Landry	Schakowsky
Cohen	Larson (CT)	Schiff
Conyers	Lee (CA)	Schwartz
Costello	Levin	Schweikert
Courtney	Lewis (GA)	Scott (VA)
Crowley	Loebsack	Sensenbrenner
Cummings	Lofgren, Zoe	Serrano
Davis (CA)	Lowey	Sewell
Davis (IL)	Luján	Sherman
DeFazio	Lynch	Simpson
DeGette	Mack	Speier
DeLauro	Marchant	Stark
Deutch	Markey	Sutton
Dingell	Matsui	Thompson (MS)
Doggett	McClintock	Tierney
Doyle	McCollum	Tonko
Edwards	McCotter	Tsongas
Ellison	McDermott	Van Hollen
Emerson	McGovern	Velázquez
Engel	McNerney	Visclosky
Eshoo	Meeks	Walsh (IL)
Farenthold	Michaud	Walz (MN)
Farr	Miller (NC)	Wasserman Schultz
Fattah	Miller, George	
Fleming	Moore	Waters
Frank (MA)	Murphy (CT)	Watt
Fudge	Nadler	Waxman
Gibson	Napolitano	Welch
Gohmert	Neal	Wilson (FL)
Gosar	Olver	Woolsey
Green, Al	Pallone	Yarmuth

NOT VOTING—15

Blumenauer	Hirono	Paul
Bucshon	Holden	Pence
Canseco	Maloney	Rangel
Davis (KY)	Marino	Sires
Filner	McHenry	Slaughter

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore (during the vote). There are 2 minutes remaining.

□ 1831

Mr. HOYER changed his vote from ''aye'' to ''no.''

Mr. TIPTON changed his vote from ''no'' to aye.''

So the bill was passed.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

Stated against:

Mr. FILNER. Mr. Speaker, on rollcall 192, I was away from the Capitol due to prior commitments to my constituents. Had I been present, I would have voted "no."

PERSONAL EXPLANATION

Ms. SLAUGHTER. Mr. Speaker, I was unavoidably detained and missed rollcall vote Nos. 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, and 192. Had I been present, I would have voted "aye" on rollcall vote Nos. 184, 185, 186, 187, 188, 189, 190, and 191. I would have voted "no" on rollcall vote Nos. 182, 183, and 192.

IDAHO WILDERNESS WATER RESOURCES PROTECTION ACT

The SPEAKER pro tempore. The unfinished business is the question on suspending the rules and passing the bill (H.R. 2050) to authorize the continued use of certain water diversions located on National Forest System land in the Frank Church-River of No Return Wilderness and the Selway-Bitterroot Wilderness in the State of Idaho, and for other purposes.

The Clerk read the title of the bill.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Utah (Mr. BISHOP) that the House suspend the rules and pass the bill.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill was passed.

A motion to reconsider was laid on the table.

AUTHORIZING THE CLERK TO MAKE CORRECTIONS IN ENGROSSMENT OF H.R. 3523, CYBER INTELLIGENCE SHARING AND PROTECTION ACT

Mr. ROGERS of Michigan. Mr. Speaker, I ask unanimous consent that in the engrossment of the bill, H.R. 3523, the Clerk be authorized to make such technical and conforming changes as necessary to reflect the actions of the House.

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

There was no objection.

Mr. ROGERS of Michigan. Madam Speaker, I ask unanimous consent that in the engrossment of H.R. 3523, the Clerk be authorized to make the change that I have placed at the desk.

The SPEAKER pro tempore (Mrs. NOEM). The Clerk will report.

The Clerk read as follows:

Insert ''deny access to or'' before ''degrade'' in each place it appears.

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

There was no objection.