Capuano	Heck (WA)	Norcross
Cárdenas	Higgins	O'Rourke
Carney	Himes	Pallone
Carson (IN)	Hinojosa	Pascrell
Cartwright	Honda	Pelosi
Castor (FL)	Hoyer	Perlmutter
Castro (TX)	Huffman	Peters
Chu, Judy	Israel	Pingree
Cicilline	Jackson Lee	Pocan
Clark (MA)	Jeffries	Polis
Clarke (NY)	Johnson (GA)	Price (NC)
Clay	Johnson, E. B.	Quigley
Cleaver	Jones	Rangel
Clyburn	Kaptur	Rice (NY)
Cohen	Keating	Richmond
Connolly	Kelly (IL)	Roybal-Allard
Conyers	Kennedy	Ruiz
Cooper	Kildee	Ruppersberger
Costa	Kilmer	Rush
Courtney	Kind	Ryan (OH)
Crowley	Kirkpatrick	Sánchez, Linda T.
Cummings	Kuster	Sanchez, Loretta
Davis (CA)	Langevin	Sarbanes
Davis, Danny	Larsen (WA)	Schakowsky
DeFazio	Larson (CT)	Schiff
DeGette	Lawrence	Schrader
Delaney	Lee	Scott (VA)
DeLauro	Levin	Scott, David
DelBene	Lewis	Serrano
DeSaulnier	Lieu, Ted	Sewell (AL)
Deutch	Lipinski	Sherman
Dingell	Loebsack	Sires
Doggett	Lofgren	Slaughter
Doyle, Michael F.	Lowenthal	Speier
	Lowey	Swalwell (CA)
Duckworth	Lujan Grisham (NM)	Takai
Edwards	Luján, Ben Ray (NM)	Takano
Ellison		Thompson (CA)
Engel	Lynch	Thompson (MS)
Eshoo	Maloney, Carolyn	Titus
Esty		Tonko
Farr	Maloney, Sean	Torres
Fattah	Massie	Tsongas
Foster	Matsui	Van Hollen
Frankel (FL)	McCollum	Vargas
Fudge	McDermott	Veasey
Gabbard	McGovern	Vela
Gallego	McNerney	Velázquez
Garamendi	Meeks	Visclosky
Graham	Meng	Walz
Grayson	Moore	Waters, Maxine
Green, Al	Moulton	Watson Coleman
Green, Gene	Nadler	Welch
Grijalva	Napolitano	Wilson (FL)
Gutiérrez	Nolan	Yarmuth
Hahn		

NOT VOTING—13

Brady (TX)	Murphy (FL)	Wasserman Schultz
Curbelo (FL)	Neal	
DesJarlais	Olson	Wenstrup
Graves (MO)	Payne	Yoho
Hastings	Smith (WA)	

□ 1432

So the bill was passed.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

RESIGNATION AS MEMBER OF COMMITTEE ON NATURAL RESOURCES

The SPEAKER pro tempore laid before the House the following resignation as a member of the Committee on Natural Resources:

CONGRESS OF THE UNITED STATES,
HOUSE OF REPRESENTATIVES,
Washington, DC, April 22, 2015.

Hon. JOHN BOEHNER,
Speaker of the House, The Capitol, Washington, DC.

DEAR SPEAKER BOEHNER: This letter serves as my official resignation from the House Committee on Natural Resources. It has been my pleasure serving on this Committee since being elected to Congress. Thank you and I will continue working on important priorities relating to my new appointment on the House Committee on Small Business.

Sincerely,

MARK TAKAI,
Member of Congress.

The SPEAKER pro tempore. Without objection, the resignation is accepted.

There was no objection.

ELECTING A MEMBER TO A CERTAIN STANDING COMMITTEE OF THE HOUSE OF REPRESENTATIVES

Mr. BECERRA. Mr. Speaker, by direction of the Democratic Caucus, I offer a privileged resolution and ask for its immediate consideration.

The Clerk read the resolution, as follows:

H. RES. 219

Resolved, That the following named Member be and is hereby elected to the following standing committee of the House of Representatives:

(1) COMMITTEE ON SMALL BUSINESS.—Mr. Takai.

The resolution was agreed to.

A motion to reconsider was laid on the table.

PROTECTING CYBER NETWORKS ACT

GENERAL LEAVE

Mr. NUNES. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and insert extraneous material on H.R. 1560, the Protecting Cyber Networks Act.

The SPEAKER pro tempore (Mr. RODNEY DAVIS of Illinois). Is there objection to the request of the gentleman from California?

There was no objection.

The SPEAKER pro tempore. Pursuant to House Resolution 212 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. 1560.

The Chair appoints the gentleman from Texas (Mr. MARCHANT) to preside over the Committee of the Whole.

□ 1436

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. 1560) to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes, with Mr. MARCHANT 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 California (Mr. NUNES) and the gentleman from California (Mr. SCHIFF) each will control 30 minutes.

The Chair recognizes the gentleman from California (Mr. NUNES).

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

Over the last several years, cyber attacks have become a pressing concern for the United States. Anthem, Home Depot, Sony, Target, JPMorgan Chase, and other companies have been subject to major attacks, resulting in the compromise of personal information of employees and customers alike.

Cyber thieves, whether hostile foreign agents or money-seeking criminals, have stolen credit card numbers, accessed medical records, leaked proprietary information, and published confidential emails affecting tens of millions of Americans. This situation cannot continue.

The House has passed cybersecurity information-sharing legislation with strong majorities in the past two Congresses. The gentleman from California, Ranking Member SCHIFF, and I have continued this bipartisan tradition, working closely together to draft a bill that will increase the security of our networks while protecting users' privacy.

I see the gentleman from Maryland (Mr. RUPPERSBERGER) is here. He sponsored this legislation last time, along with the gentleman from Michigan, Chairman Rogers, who is now retired, but I do want to give them a special thanks and gratitude.

I hope that we can get this bill across the floor this year.

We have also worked closely with leadership—the gentleman from Texas, Chairman MCCAUL; the gentleman from Virginia, Chairman GOODLATTE—and the Senate Intelligence Committee to ensure that our bills complement each other.

The Protecting Cyber Networks Act addresses a core problem in our digital security infrastructure. Because of legal ambiguities, many companies are afraid to share information about cyber threats with each other or with the government. If a company sees some threat or attack, this bill will allow the company to quickly report information about the problem without fearing a lawsuit so that other companies can take measures to protect themselves.

The bill encourages three kinds of sharing: private-to-private, government-to-private, and private-to-government. In that third scenario, the bill allows companies to share cyber threat information with a variety of government agencies. If banks are comfortable sharing with the Treasury Department, they can share with Treasury. If utilities prefer sharing with the Department of Energy, they can share with Energy. If companies want to share with the Department of Homeland Security, the Justice Department, or the Commerce Department, they can share with them.

The only sharing that this bill does not encourage is direct sharing to the Department of Defense or the National Security Agency. Companies can still share with DOD and NSA, but they will not receive any new liability protections.

This bill does not provide the government with any new surveillance authorities. To the contrary, it includes robust privacy protections. It only authorizes the sharing of cyber threat indicators and defensive measures: technical information like malware signatures and malicious code.

Before companies share with the Federal Government, they must remove all personal information. If companies don't follow those requirements, there is no liability protection. Furthermore, a government agency that receives the information must scrub it a second time. This will ensure all personal information has been removed. Only then can the information be forwarded to other Federal agencies.

Finally, the bill provides for strong public and congressional oversight by requiring a detailed biennial inspectors general report relating to the government's receipt, use, and dissemination of cyber threat indicators. The Privacy and Civil Liberties Oversight Board must also submit a biennial report on the privacy and civil liberties impact of the bill.

The increasing pace and scope of cyber attacks cannot be ignored. This bill will strengthen our digital defenses so that American consumers and businesses will not be put at the mercy of cyber criminals. I look forward to passing this legislation.

I reserve the balance of my time.

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

I rise in support of H.R. 1560, the Protecting Cyber Networks Act. At some point, we need to stop just hearing about cyber attacks that steal our most valuable trade secrets and our most private information and actually do something to stop it. At some point, we need to stop talking about the next Sony, the next Anthem, the next Target, the next JPMorgan Chase, and the next State Department hack and actually pass a bill that will help ensure that there will be no next cyber attack.

A few weeks back, the House Intelligence Committee held an open hearing on the cyber threat to America's private sector. We heard from our witnesses that their businesses are cyber attacked billions of times a day—not thousands, not millions, but billions.

The threat to our economy, our jobs, and our privacy from not acting is massive, and it is certain. We see it happening all around us. So we must act now. That is why I am proud to support this bill.

The Protecting Cyber Networks Act provides for voluntary information sharing of cyber threats between and among the private and public sectors. It does what no executive order can do: it incentivizes cyber threat information sharing by providing limited liability protection. Now companies can pool their resources and say to one another: I found this malicious code or this virus in my system; you need to protect yourself against it as well. And now the government can better warn companies of an impending cyber attack, just as it can for an approaching hurricane or an impending flu outbreak.

But let me be very clear about this: to get the liability protection, a company that chooses to participate must remove any unrelated private information prior to sharing. This is something privacy advocates and I called for when previous information-sharing bills came before the House.

Unlike prior bills, this measure requires the private sector to strip out private information. In fact, the bill has two, not one, privacy scrubs. The first happens when a company shares with another company or the Federal Government, and the second happens when the Federal Government shares the information further. This bill even holds the government directly liable if it doesn't do what it is required to do.

Second, to get the liability protection, a private company wishing to share with the Federal Government must go through a civilian portal. To be clear: a company can't go directly to the DOD or NSA and get the bill's liability protection.

The lack of a civilian portal in previous bills was another key privacy group criticism, and this bill has resolved that issue, too. In fact, of the five main criticisms of prior cyber bills, this bill has resolved each of them. It has private sector privacy stripping of information. It has a civilian portal. It also has narrow restrictions on what the government can use that shared cyber threat information for. Gone is a national security use provision. Gone is a vague terrorism use provision. And what is left is only the most narrow of uses: to prevent cyber attacks, to prevent the loss of life, to prevent serious harm to a child, and to prevent other serious felonies.

□ 1445

Gone, too, is any question of whether offensive countermeasures or hack back is authorized. This bill makes clear that you cannot take anything but defensive actions to protect your networks and data.

And, lest anyone be confused, Mr. Chairman, this bill makes clear in black-and-white legislative text that nothing in the bill authorizes government surveillance in this act—nothing.

What this bill does is authorize voluntary, private sector sharing of cyber threat information, and it allows the government to be able to quickly share threat information with the private sector, just as we need a CDC to put out timely warnings and advice on how to counteract this year's flu strain or how to prevent a local disease from becoming an epidemic. In addition, the bill requires strong privacy and civil liberties guidelines and intense reporting requirements.

The bill before us today strikes the right balance between securing our networks and protecting our privacy, and addresses the privacy concerns that I, among others, raised last session. However, there are still some improvements that are yet to be made as the bill moves forward. In particular, we need to further clarify that our liability protection only extends to those who act, or fail to act, reasonably.

Before closing, I want to thank Chairman NUNES for his leadership and for working so hard on this bill. It has been a great pleasure to work with you, Mr. Chairman. I am grateful for all of the hours, energy, and talent that you and your staff have put in to making this bill successful. I want to thank all the members of HPSCI as well as the Judiciary Committee and the Homeland Security Committee for working together on this. We had many differences in opinion, and we still have some, but we kept our eyes firmly on what is best for the American people as a whole. With that, we found ways to come together and produce a stronger bill.

Mr. Chairman, I hope we can continue to work together as well with the Senate and with the White House and all the stakeholders to produce an even stronger bill for the President to sign into law.

I also want to acknowledge the leadership of our predecessors, DUTCH RUPPERSBERGER and former HPSCI Chairman Mike Rogers. We have come this far in part because of the good work they did in the last couple of sessions. I also want to thank all those who came in to speak with us and provide their input in making this a better bill.

Every day we delay more privacy is stolen, more jobs are lost, and more economic harm is done. Let's stop sitting by and watching all of this happen. Let's do something. Let's do what this administration has urged us to do and pass this bill. Let's do it now. I reserve the balance of my time.

Mr. NUNES. Madam Chair, at this time I would like to yield 3 minutes to the gentleman from Georgia (Mr. WESTMORELAND), who also is the chairman of the Subcommittee on NSA and Cybersecurity for the House Intelligence Committee.

Mr. WESTMORELAND. Thank you, Chairman NUNES.

Madam Chairman, today I rise in support of H.R. 1560, the Protecting Cyber Networks Act. The bill encourages and protects information sharing on cyber threats between private companies and the government and private companies. The bill safeguards personally identifiable information from being exchanged during the process by requiring private companies and the government to both make sure that no private information is exchanged.

My home State of Georgia is home to many companies that deal with and secure sensitive data on a daily basis, and they are constantly looking for better ways to protect their networks.

After recent cyber attacks against American businesses, I have spoken to industry leaders from Georgia and

across the Nation about how we can make information sharing between the industries and the government stronger to better protect our Nation.

Cyberterrorism is the new battlefield, and adapting to this warfare is crucial to eliminating these threats. By allowing American businesses to alert other companies and the government of specific threats, and only the threats, the Protecting Cyber Networks Act can help shut down the cybercriminals from stealing sensitive information or causing devastating damage to our networks.

The Protecting Cyber Networks Act is a bipartisan step forward in protecting businesses and citizens from being the next victim of a cyber attack. This bill helps devastating cyber attacks from going unnoticed or only being shared months after the attack.

Madam Chairman, I would like to thank Chairman NUNES; Ranking Member SCHIFF; the ranking member on the subcommittee, Mr. HIMES; and Mr. RUPPERSBERGER for all the work that he has put into this, as well as former Chairman Rogers. I ask for a ''yea'' vote on this.

Mr. SCHIFF. Madam Chair, it is a pleasure to yield 2 minutes to the gentleman from Maryland (Mr. RUPPERSBERGER), the former ranking member of the Intelligence Committee.

Mr. RUPPERSBERGER. Madam Chairman, I rise in support of the bipartisan Protecting Cyber Networks Act and want to thank the members of the House Intelligence Committee for continuing to prioritize our Nation's security over partisan rhetoric. I do want to say this: I want to thank Chairman NUNES and also Ranking Member SCHIFF for acknowledging Chairman Rogers and me, but I want to remind you that it was a team approach, and you two were very active in helping to bring this bill here today as we did before. So thank you for your leadership. It is well worth it, and it is refreshing to see this bipartisanship.

Mr. NUNES. Will the gentleman yield?

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

Mr. NUNES. I thank the gentleman for yielding. I thanked you in my opening statement, Mr. RUPPERSBERGER, but without your leadership and former Chairman Rogers' leadership on this bill, we would not be here today. I am encouraged not only by your past support, but then your taking the time to come down here to speak on this bill I think says a lot about you and your commitment to our national security and the security of our cyber networks. So thank you.

Mr. RUPPERSBERGER. Thank you, again, and thank you for your leadership. Now, this legislation is very similar to the bill that Chairman Rogers and I introduced to promote information sharing between the private and public sectors, which is the single most important thing we can do to combat increasingly aggressive cyber attacks.

Experts believe these attacks are costing American corporations billions of dollars each year. Target, Home Depot, and CareFirst are only the beginning. With Sony, we saw the first destructive attack in our country. It is only a matter of time before our critical infrastructure is targeted. What would happen if someone were to take out our electrical grid or 911 call centers or air traffic control? It goes on and on.

Voluntary information sharing among companies helps our companies defend themselves. Voluntary, two-way information sharing with the Federal Government helps improve our ability to protect America against foreign cyber threats by getting out more and better information faster.

There are some concerns I have, as anyone has in any bill, between the bill and the bill Chairman Rogers and I introduced which passed the House.

The Acting CHAIR (Ms. FOXX). The time of the gentleman has expired.

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

Mr. RUPPERSBERGER. However, I feel it is important to reach consensus and move this issue forward now. Our country continues to be cyber attacked. We are under attack as I speak. To do nothing is not an option.

I want to thank again the leadership of Chairman NUNES and Ranking Member SCHIFF for their leadership and for the entire committee coming together for this bill, and I ask my colleagues to support it.

Mr. NUNES. Madam Chair, at this time I yield 5 minutes to the gentleman from Texas (Mr. MCCAUL), the chairman of the Homeland Security Committee, who, without his strong leadership and support, we wouldn't be at this juncture today getting a bill passed today and tomorrow that will hopefully become law.

Mr. MCCAUL. Madam Chair, I rise today in strong support of H.R. 1560, the Protecting Cyber Networks Act. I would like to first thank Chairman NUNES for his great leadership and collaboration with my committee and Judiciary on this bill, and also the ranking member, ADAM SCHIFF, a good friend as well, for his great work in the direction that this bill has gone. I think it has gone in the right direction. Also I know former Ranking Member DUTCH RUPPERSBERGER was here. I want to thank him for his leadership over the many years on this important issue of cybersecurity.

Madam Chair, this legislation comes at a critical time of rising cyber threats and attacks on our digital networks. Cyber breaches and attacks are affecting Americans' privacy, security, and prosperity. Individuals are having their most private information compromised. Businesses are seeing their intellectual property stolen and their networks damaged.

The Federal Government's sensitive information is being targeted. The country's critical infrastructure is being probed by foreign enemies.

Detecting and defending against these digital assaults requires timely and robust information sharing between the public and private sectors. This exchange of data is crucial to connecting the dots, identifying cyber attacks, and shutting them down.

The Protecting Cyber Networks Act will enable private companies to share cyber threat information on a voluntary basis with the Federal Government. This bill provides essential liability protection for sharing cyber threat indicators through trusted civilian agency portals.

Again, Madam Chair, I commend Chairman NUNES for his important work on this bill and thank him for his great partnership in working together to have these two complementary bills, as tomorrow I will bring to the floor a pro-security, pro-privacy bill, the National Cybersecurity Protection Advancement Act of 2015, which further reinforces the role of the Department of Homeland Security's National Cybersecurity and Communications Integration Center as the hub for cyber threat information sharing.

Chairman NUNES and I have worked in lockstep to remove obstacles preventing greater cyber threat information sharing across the private and public sectors. I commend the staff on both sides of the aisle, who have operated in tandem as we crafted these cybersecurity bills. I would also like to acknowledge Chairman GOODLATTE for devising the House's standard liability exemption language for this week's cybersecurity bill.

These bills represent a unified front in the House for strengthening cybersecurity while ensuring Americans' privacy, and I urge my colleagues to support this measure.

Mr. SCHIFF. Madam Chair, it gives me great pleasure to yield 3 minutes to Mr. HIMES, one of our subcommittee ranking members on the Intelligence Committee and the Representative from Connecticut.

Mr. HIMES. Madam Chairwoman, I would like to thank my friend from California for yielding time and start by saying that I am thrilled to be standing here to urge support for the Protecting Cyber Networks Act. I would like to thank and congratulate Chairman NUNES, Ranking Member SCHIFF, and the chairman of the subcommittee on which I serve as ranking member, Mr. WESTMORELAND, for coming together at a time when this Congress is accused, often rightly so, of being dysfunctional to take a very substantial step to secure the networks on which so much of our lives today depend.

As ranking member of the Cybersecurity Subcommittee, my daily travels every single day expose me to people who say the single most important thing we as a Congress can do today to advance the security of our networks, to protect Americans, their financial records, their health records and, of course, even more ominously, to protect them against potential attack

against our utilities and any sort of thing that our antagonists around the world would seek to do to us, the single most important thing we can do is to do what we are doing today, which is to set up a rubric whereby the very good people within the private sector who focus on this day in and day out can communicate threats to each other and communicate with the experts within the United States Government to work as a team to counter very, very serious threats. This rubric has been set up with ample attention and good attention to the very legitimate privacy claims and the liberties that we all take so seriously.

The stakes are high. We saw what happened at Sony. We saw what happened at Anthem. We know all the attacks that have been leveled internationally that destroyed computers. This is the reality that we live with, and this is a very big step, an information-sharing protocol that will counter those who wish us ill.

I would note that the privacy protections in this bill are considerably better, as the chairman and ranking member have pointed out, than those that were in the bill of the last Congress. The objections of those who are focused on privacy have been dealt with point by point. And while I won't say that the bill is perfect, this bill does what it needs to do to protect the privacy of the American people by obligating everyone to work hard to scrub personally identifiable information from any code, any information that is exchanged.

I have learned in my 6 years here that we don't produce perfection, and it is my hope that as this bill proceeds through the legislative path that we will work even harder to make sure we are very clear about definitions and, in fact, are protecting the privacy rights of Americans as best as we can. But in the meantime we have taken a very big step forward in a bipartisan fashion in a way that will make America, its people, and its networks more secure. For that, I am grateful to the leadership and urge support of the Protecting Cyber Networks Act.

Mr. NUNES. Madam Chair, I continue to reserve the balance of my time.

Mr. SCHIFF. Madam Chairman, I yield 3 minutes to the gentleman from California (Mr. SWALWELL), another of our ranking members on the Intelligence Committee and a colleague from California.

□ 1500

Mr. SWALWELL of California. Madam Chair, I want to thank our ranking member and also the chair for bringing forward this bipartisan and necessary legislation.

As we speak right now, Americans are under attack, and these attacks are not coming in the form of anything that we have been used to before. People are not kicking down front doors of homes and businesses; instead, they are attacking us through our networks. Our bank accounts, our health care records, our social media accounts, our cell phones, all are being hacked every day.

CNN reported that, in 2014, half of the Nation's adults were hacked. The examples are voluminous: 70 million Target customers were hacked; 56 million Home Depot customers were hacked; 4.6 million Snapchat users were hacked. This is Snapchat, which is supposed to be an impenetrable account that allows data to come in and disappear. They were hacked. Hackings are happening every day. Our privacy is under attack.

The problem, today, there is virtually zero relationship between private industry and government—private industry, which has about 85 percent of the networks, and government, which has about 15 percent of the networks but has vast resources that can help protect individuals against attacks.

Our government has a duty, a responsibility, to protect the American people, and that is what this bill seeks to do. It does it in a number of ways.

First and foremost, this is a voluntary program that is being created. No business is required to turn over their breach or hack information to the government; instead, there is a format, a procedure, that is now in place that will incentivize them to work with the government to identify in a way that strips out, through a number of protections, personal identifying information.

The first way that it is stripped out is, when the business that has been hacked reports to a civilian agency, they must scrub the personal identifying information; but that is not the only way that that information is scrubbed.

Once the government agency receives this personal identifying information, again, before it can be used or forwarded anywhere else in the government, it, again, must be scrubbed—two protections against personal identifying information being used.

Now, should any personal identifying information be passed along to the government, this bill provides a right of action, civil recourse for any individual who is wronged to sue the government. There is also an oversight committee, a biannual inspector general report that must be presented to Congress that would report on any privacy violations that occur.

Madam Chair, the American people, day after day, are either learning that they have been hacked or someone they know has been hacked. This will continue to have a devastating effect on our economy and, as my colleague from Connecticut alluded to, perhaps our public utilities if we do not act.

I urge support of this for my colleagues, and I thank the chairman and the ranking member for the hard work they have done.

Mr. NUNES. Madam Chair, I continue to reserve the balance of my time.

Mr. SCHIFF. Madam Chair, I yield 3 minutes to the gentlewoman from Alabama (Ms. SEWELL), another one of the ranking members on the Intelligence Committee and a great Member.

Ms. SEWELL of Alabama. Madam Chair, I would like to thank Ranking Member ADAM SCHIFF, as well as our chair, Chairman NUNES, for your leadership on this matter.

Today, I rise in support of H.R. 1560, the Protecting Cyber Networks Act, a bill that I am proud to be an original cosponsor, a bill that was unanimously voted out of our committee, the Intel Committee.

Again, I want to commend both the chairman and the ranking member for their leadership. It is an honor to serve on that committee where we really try, on a daily basis, to be bipartisan in our efforts to protect the homeland and to secure our national security.

This critical bill is bipartisan legislation, which encourages the private sector to share cyber threat information, which will ultimately help prevent future attacks. It seems like we are always hearing about another company being hit with cyber attacks.

These attacks cost our economy billions of dollars each year, and it threatens our national security and jeopardizes every American's sensitive, personal, and financial information.

This bill takes a very important step towards addressing this emerging national security threat without compromising the privacy of American citizens.

Fostering an environment where companies can voluntarily share information with each other helps American businesses defend themselves against harmful cyber attacks and helps them protect consumer information and privacy.

Additionally, two-way information sharing with the Federal Government helps improve the Federal Government's ability to protect all Americans against foreign cyber threats by disseminating vital information in a more timely and efficient manner.

I know some continue to criticize this cyber bill and all cyber bills as violating privacy, but I must assure you, Madam Chair, that this bill is a vast improvement over the CISPA bill that was entered and passed this House last term.

This bill includes many more privacy protections that weren't in the original bill, the most important of which is the requirement for two scrubs of private information, one by the private sector before sharing that information and one by the government before sharing it further.

There is also now a civilian portal—no direct sharing with NSA—a very narrow set of government use provisions, and a clear and legislative prohibition against such surveillance. Let me repeat: no provision of this bill provides any surveillance authorities.

I am encouraged by the strong showing of bipartisanship as we work together to address the emerging threats

to our national security. I urge my colleagues to join those of us who are members of the Intel Committee, as well as this administration has said that it also encourages a vote in support of this bill.

I urge my colleagues to support the efforts and vote ''yes'' on H.R. 1560.

Mr. NUNES. Madam Chair, at this time, I yield 2 minutes to the gentleman from Michigan (Mr. TROTT).

Mr. TROTT. Madam Chair, I want to thank the gentleman from California for allowing me to speak in support of this bill.

Today, I rise concerned about the need for stronger cybersecurity efforts in our country. We live in a world where personal data flows through the Internet with great speed and data about people is gathered in an instant. The use of social media has opened up our lives to anyone with a computing device, and this is the same world where hackers steal millions of personal records from people in our districts.

I would venture to guess that most Members of Congress have been affected by hackers. Internet criminals pose dire threats to our governments on the local, State, and Federal level. The Federal Government has extensive resources to put up a fight, but our local governments and municipalities do not.

In response, five southeast Michigan counties—Livingston, Monroe, Oakland, Washtenaw, and Wayne—and the State of Michigan came together to build the Cyber Security Assessment for Everyone. CySAFE, as it is known, provides a strong point for governments to begin assessing their cybersecurity needs and taking steps to respond to attacks. The assessment is a simple Excel download located at www.g2gmarket.com.

Madam Chair, I commend these local Michigan governments for committing the resources to develop such a tool. I encourage all of my colleagues to promote the use of CySAFE and to work together to find the right solutions to fight cyber crime, starting with passing H.R. 1560.

Mr. SCHIFF. Madam Chair, I am pleased to yield 2 minutes to the gentleman from Rhode Island (Mr. LANGEVIN), who is a former member of the Intelligence Committee and one of the Congress' leading experts on cyber matters.

Mr. LANGEVIN. Madam Chair, I thank the gentleman for yielding.

Madam Chair, this has been a long time in coming. When I served on the Intelligence Committee the past two Congresses, I worked very closely with Chairman Rogers and Ranking Member RUPPERSBERGER on CISPA, and their legacy is very evident in this fine bill.

I would, however, like to commend Chairman NUNES and Ranking Member SCHIFF for rising to the challenge as the new leaders of the House Permanent Select Committee on Intelligence and producing an even better product, particularly with regard to privacy protections.

PCNA, as it is known, also provides statutory authorization for the CTIIC, an important new center the President has created to provide comprehensive assessments of cyber threats.

This bill before us certainly isn't perfect. The liability protections, while generally narrow, could still be construed to project a company's failure to act on threat indicators. It is important that my friends in this Chamber understand that information sharing is not a silver bullet.

There will still be important work to be done to improve our Nation's cyber defenses, but I can say, with great confidence, passing an information-sharing bill will get us significantly closer to being much more secure in cyberspace than where we are right now, particularly when it comes to protecting critical infrastructure.

However, after studying this issue for the better part of a decade, I can firmly say that this bill marks a meaningful step forward.

Let me, again, congratulate the chairman and the ranking member for continuing with this bipartisan spirit that has long animated the Intelligence Committee's cybersecurity work.

I urge my colleagues to support the bill.

Mr. NUNES. Madam Chair, I reserve the balance of my time.

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

Every moment we wait equals another Social Security number stolen, another checking account hacked, another invaluable trade secret pilfered, and another job lost. This is certain. We see it every day.

Many of us and our constituents, both individuals and businesses, have been the victim of a cyber crime. Whether it is identity theft, the hacking of our email or Facebook accounts, or the loss of our privacy, when our health insurance company is breached, we have our privacy invaded.

All of us are certainly paying higher fees to compensate for the billions of dollars our businesses lose to cyber hacking and to the costs of preventing future cyber attacks. The problem is only getting worse. As our cars, our phones, our home security systems, our Internet banking, our electronic health records, our web-based baby monitors all get smarter, they also get more vulnerable.

This isn't speculation. This is happening today. It is happening right now. On the time that we have been on the floor discussing this cyber bill, billions of additional hacking attempts have been made.

Here, we have the opportunity to help stop this scourge of cyber hacking. We need to encourage cyber threat information sharing by passing the Protecting Cyber Networks Act today and then not resting until it improves on its way to the President's desk for signature.

I urge my colleagues to vote for this important measure. It is a bill that will help protect America's most valuable and private information, while itself protecting privacy and civil liberties to a degree far in advance of where prior legislation has gone. I and my colleagues have made sure of that, and we will continue to do so as the bill advances.

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

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

I will close by just taking a few moments to thank my ranking member and colleague from California (Mr. SCHIFF) for his fine work on this product.

I also would be remiss not to thank, on both sides of the aisle, the staff that have worked hours and hours and hours to make the legislation from last Congress even better and then, as Mr. MCCAUL said, to work with the Judiciary Committee and the Homeland Security Committee so that we have a product that I think is much better than the product that we have had in the past.

We have been in consultations with the United States Senate. They have passed their bill out of committee. We look forward to, hopefully, their passing a bill off the Senate floor so that we can get to a conference.

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

Mr. VAN HOLLEN. Madam Chair, I rise today to oppose to H.R. 1560, the Protecting Cyber Network Act (PCNA). While I commend Chairman NUNES and Ranking Member SCHIFF for crafting a bill that improves upon the cybersecurity legislation this body has previously voted on, I cannot support it in its current form.

Despite addressing many of the reservations I had when we voted on the Cyber Intelligence Sharing and Protection Act (CISPA) last Congress, I have concerns about the ambiguous liability provisions in this legislation. While companies should have some legal protection, this bill gives liability protections to companies so long as they share or receive information ''in accordance with the Act.'' It would grant immunity to companies for simply putting forth a ''good faith'' effort when reporting security threats and sharing consumer data with the government and other companies. For example, companies would receive liability protection even if they fail to act on threat information in a timely manner. The unintended effect of these murky liability provisions is that companies would not have the same incentive to report security threats and protect their consumers' privacy. I was disappointed that Republicans did not allow a vote on two amendments offered by Rep. RICHMOND than would have addressed these overbroad liability provisions.

Our country faces cyber-network attacks each day which threaten our national security and our economy. I strongly believe that we must take steps to protect against these cyber threats while not sacrificing our privacy and civil liberties. Should this bill pass the House,

I hope that many of the loopholes can be resolved with the Senate, but as it stands today I cannot support it.

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.

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 recommended by the Permanent Select Committee on Intelligence printed in the bill. The committee amendment in the nature of a substitute shall be considered as read.

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

H.R. 1560

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Protecting Cyber Networks Act''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

SEC. 2. SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT WITH NON-FEDERAL ENTITIES.

(a) IN GENERAL.—Title I of the National Security Act of 1947 (50 U.S.C. 3021 et seq.) is amended by inserting after section 110 (50 U.S.C. 3045) the following new section:

''SEC. 111. SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT WITH NON-FEDERAL ENTITIES.

''(a) SHARING BY THE FEDERAL GOVERNMENT.—

''(1) IN GENERAL.—Consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties, the Director of National Intelligence, in consultation with the heads of the other appropriate Federal entities, shall develop and promulgate procedures to facilitate and promote—

''(A) the timely sharing of classified cyber threat indicators in the possession of the Federal Government with representatives of relevant non-Federal entities with appropriate security clearances;

''(B) the timely sharing with relevant non-Federal entities of cyber threat indicators in the possession of the Federal Government that may be declassified and shared at an unclassified level; and

''(C) the sharing with non-Federal entities, if appropriate, of information in the possession of the Federal Government about imminent or ongoing cybersecurity threats to such entities to prevent or mitigate adverse impacts from such cybersecurity threats.

''(2) DEVELOPMENT OF PROCEDURES.—The procedures developed and promulgated under paragraph (1) shall—

''(A) ensure the Federal Government has and maintains the capability to share cyber threat indicators in real time consistent with the protection of classified information;

''(B) incorporate, to the greatest extent practicable, existing processes and existing roles and responsibilities of Federal and non-Federal entities for information sharing by the Federal Government, including sector-specific information sharing and analysis centers;

''(C) include procedures for notifying non-Federal entities that have received a cyber threat indicator from a Federal entity in accordance with this Act that is known or determined to be in error or in contravention of the requirements of this section, the Protecting Cyber Networks Act, or the amendments made by such Act or another provision of Federal law or policy of such error or contravention;

''(D) include requirements for Federal entities receiving a cyber threat indicator or defensive measure to implement appropriate security controls to protect against unauthorized access to, or acquisition of, such cyber threat indicator or defensive measure;

''(E) include procedures that require Federal entities, prior to the sharing of a cyber threat indicator, to—

''(i) review such cyber threat indicator to assess whether such cyber threat indicator, in contravention of the requirement under section 3(d)(2) of the Protecting Cyber Networks Act, contains any information that such Federal entity knows at the time of sharing to be personal information of or information identifying a specific person not directly related to a cybersecurity threat and remove such information; or

''(ii) implement a technical capability configured to remove or exclude any personal information of or information identifying a specific person not directly related to a cybersecurity threat; and

''(F) include procedures to promote the efficient granting of security clearances to appropriate representatives of non-Federal entities.

''(b) DEFINITIONS.—In this section, the terms 'appropriate Federal entities', 'cyber threat indicator', 'defensive measure', 'Federal entity', and 'non-Federal entity' have the meaning given such terms in section 11 of the Protecting Cyber Networks Act.''.

(b) SUBMITTAL TO CONGRESS.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of the other appropriate Federal entities, shall submit to Congress the procedures required by section 111(a) of the National Security Act of 1947, as inserted by subsection (a) of this section.

(c) TABLE OF CONTENTS AMENDMENT.—The table of contents in the first section of the National Security Act of 1947 is amended by inserting after the item relating to section 110 the following new item:

''Sec. 111. Sharing of cyber threat indicators and defensive measures by the Federal Government with non-Federal entities.''.

SEC. 3. AUTHORIZATIONS FOR PREVENTING, DETECTING, ANALYZING, AND MITIGATING CYBERSECURITY THREATS.

(a) AUTHORIZATION FOR PRIVATE-SECTOR DEFENSIVE MONITORING.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for a cybersecurity purpose, monitor—

(A) an information system of such private entity;

(B) an information system of a non-Federal entity or a Federal entity, upon the written authorization of such non-Federal entity or such Federal entity; and

(C) information that is stored on, processed by, or transiting an information system monitored by the private entity under this paragraph.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed to—

(A) authorize the monitoring of an information system, or the use of any information obtained through such monitoring, other than as provided in this Act;

(B) authorize the Federal Government to conduct surveillance of any person; or

(C) limit otherwise lawful activity.

(b) AUTHORIZATION FOR OPERATION OF DEFENSIVE MEASURES.—

(1) IN GENERAL.—Except as provided in paragraph (2) and notwithstanding any other provision of law, a private entity may, for a cybersecurity purpose, operate a defensive measure that is operated on and is limited to—

(A) an information system of such private entity to protect the rights or property of the private entity; and

(B) an information system of a non-Federal entity or a Federal entity upon written authorization of such non-Federal entity or such Federal entity for operation of such defensive measure to protect the rights or property of such private entity, such non-Federal entity, or such Federal entity.

(2) LIMITATION.—The authority provided in paragraph (1) does not include the intentional or reckless operation of any defensive measure that destroys, renders unusable or inaccessible (in whole or in part), substantially harms, or initiates a new action, process, or procedure on an information system or information stored on, processed by, or transiting such information system not owned by—

(A) the private entity operating such defensive measure; or

(B) a non-Federal entity or a Federal entity that has provided written authorization to that private entity for operation of such defensive measure on the information system or information of the entity in accordance with this subsection.

(3) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the use of a defensive measure other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

(c) AUTHORIZATION FOR SHARING OR RECEIVING CYBER THREAT INDICATORS OR DEFENSIVE MEASURES.—

(1) IN GENERAL.—Except as provided in paragraph (2) and notwithstanding any other provision of law, a non-Federal entity may, for a cybersecurity purpose and consistent with the requirement under subsection (d)(2) to remove personal information of or information identifying a specific person not directly related to a cybersecurity threat and the protection of classified information—

(A) share a lawfully obtained cyber threat indicator or defensive measure with any other non-Federal entity or an appropriate Federal entity (other than the Department of Defense or any component of the Department, including the National Security Agency); and

(B) receive a cyber threat indicator or defensive measure from any other non-Federal entity or an appropriate Federal entity.

(2) LAWFUL RESTRICTION.—A non-Federal entity receiving a cyber threat indicator or defensive measure from another non-Federal entity or a Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator or defensive measure by the sharing non-Federal entity or Federal entity.

(3) CONSTRUCTION.—Nothing in this subsection shall be construed to—

(A) authorize the sharing or receiving of a cyber threat indicator or defensive measure other than as provided in this subsection;

(B) authorize the sharing or receiving of classified information by or with any person not authorized to access such classified information;

(C) prohibit any Federal entity from engaging in formal or informal technical discussion regarding cyber threat indicators or defensive measures with a non-Federal entity or from providing technical assistance to address vulnerabilities or mitigate threats at the request of such an entity;

(D) limit otherwise lawful activity;

(E) prohibit a non-Federal entity, if authorized by applicable law or regulation other than this Act, from sharing a cyber threat indicator or defensive measure with the Department of Defense or any component of the Department, including the National Security Agency; or

(F) authorize the Federal Government to conduct surveillance of any person.

(d) PROTECTION AND USE OF INFORMATION.—

(1) SECURITY OF INFORMATION.—A non-Federal entity monitoring an information system, operating a defensive measure, or providing or receiving a cyber threat indicator or defensive measure under this section shall implement an appropriate security control to protect against unauthorized access to, or acquisition of, such cyber threat indicator or defensive measure.

(2) REMOVAL OF CERTAIN PERSONAL INFORMATION.—A non-Federal entity sharing a cyber threat indicator pursuant to this Act shall, prior to such sharing, take reasonable efforts to—

(A) review such cyber threat indicator to assess whether such cyber threat indicator contains any information that the non-Federal entity reasonably believes at the time of sharing to be personal information of or information identifying a specific person not directly related to a cybersecurity threat and remove such information; or

(B) implement a technical capability configured to remove any information contained within such indicator that the non-Federal entity reasonably believes at the time of sharing to be personal information of or information identifying a specific person not directly related to a cybersecurity threat.

(3) USE OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY NON-FEDERAL ENTITIES.—A non-Federal entity may, for a cybersecurity purpose—

(A) use a cyber threat indicator or defensive measure shared or received under this section to monitor or operate a defensive measure on—

(i) an information system of such non-Federal entity; or

(ii) an information system of another non-Federal entity or a Federal entity upon the written authorization of that other non-Federal entity or that Federal entity; and

(B) otherwise use, retain, and further share such cyber threat indicator or defensive measure subject to—

(i) an otherwise lawful restriction placed by the sharing non-Federal entity or Federal entity on such cyber threat indicator or defensive measure; or

(ii) an otherwise applicable provision of law.

(4) USE OF CYBER THREAT INDICATORS BY STATE, TRIBAL, OR LOCAL GOVERNMENT.—

(A) LAW ENFORCEMENT USE.—A State, tribal, or local government may use a cyber threat indicator shared with such State, tribal, or local government for the purposes described in clauses (i), (ii), and (iii) of section 4(d)(5)(A).

(B) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator shared with a State, tribal, or local government under this section shall be—

(i) deemed voluntarily shared information; and

(ii) exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records, except as otherwise required by applicable State, tribal, or local law requiring disclosure in any criminal prosecution.

(e) NO RIGHT OR BENEFIT.—The sharing of a cyber threat indicator with a non-Federal entity under this Act shall not create a right or benefit to similar information by such non-Federal entity or any other non-Federal entity.

SEC. 4. SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH APPROPRIATE FEDERAL ENTITIES OTHER THAN THE DEPARTMENT OF DEFENSE OR THE NATIONAL SECURITY AGENCY.

(a) REQUIREMENT FOR POLICIES AND PROCEDURES.—

(1) IN GENERAL.—Section 111 of the National Security Act of 1947, as inserted by section 2 of this Act, is amended—

(A) by redesignating subsection (b) as subsection (c); and

(B) by inserting after subsection (a) the following new subsection:

''(b) POLICIES AND PROCEDURES FOR SHARING WITH THE APPROPRIATE FEDERAL ENTITIES OTHER THAN THE DEPARTMENT OF DEFENSE OR THE NATIONAL SECURITY AGENCY.—

''(1) ESTABLISHMENT.—The President shall develop and submit to Congress policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government.

''(2) REQUIREMENTS CONCERNING POLICIES AND PROCEDURES.—The policies and procedures required under paragraph (1) shall—

''(A) be developed in accordance with the privacy and civil liberties guidelines required under section 4(b) of the Protecting Cyber Networks Act;

''(B) ensure that—

''(i) a cyber threat indicator shared by a non-Federal entity with an appropriate Federal entity (other than the Department of Defense or any component of the Department, including the National Security Agency) pursuant to section 3 of such Act is shared in real-time with all of the appropriate Federal entities (including all relevant components thereof);

''(ii) the sharing of such cyber threat indicator with appropriate Federal entities is not subject to any delay, modification, or any other action without good cause that could impede receipt by all of the appropriate Federal entities; and

''(iii) such cyber threat indicator is provided to each other Federal entity to which such cyber threat indicator is relevant; and

''(C) ensure there—

''(i) is an audit capability; and

''(ii) are appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully use a cyber threat indicator or defense measure shared with the Federal Government by a non-Federal entity under the Protecting Cyber Networks Act other than in accordance with this section and such Act.''.

(2) SUBMISSION.—The President shall submit to Congress—

(A) not later than 90 days after the date of the enactment of this Act, interim policies and procedures required under section 111(b)(1) of the National Security Act of 1947, as inserted by paragraph (1) of this section; and

(B) not later than 180 days after such date, final policies and procedures required under such section 111(b)(1).

(b) PRIVACY AND CIVIL LIBERTIES.—

(1) GUIDELINES OF ATTORNEY GENERAL.—The Attorney General, in consultation with the heads of the other appropriate Federal agencies and with officers designated under section 1062 of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee–1), shall develop and periodically review guidelines relating to privacy and civil liberties that govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in accordance with this Act and the amendments made by this Act.

(2) CONTENT.—The guidelines developed and reviewed under paragraph (1) shall, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats—

(A) limit the impact on privacy and civil liberties of activities by the Federal Government under this Act, including guidelines to ensure that personal information of or information identifying specific persons is properly removed from information received, retained, used, or disseminated by a Federal entity in accordance with this Act or the amendments made by this Act;

(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of or information identifying specific persons, including by establishing—

(i) a process for the prompt destruction of such information that is known not to be directly related to a use for a cybersecurity purpose;

(ii) specific limitations on the length of any period in which a cyber threat indicator may be retained; and

(iii) a process to inform recipients that such indicators may only be used for a cybersecurity purpose;

(C) include requirements to safeguard cyber threat indicators containing personal information of or identifying specific persons from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines;

(D) include procedures for notifying non-Federal entities and Federal entities if information received pursuant to this section is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator;

(E) be consistent with any other applicable provisions of law and the fair information practice principles set forth in appendix A of the document entitled ''National Strategy for Trusted Identities in Cyberspace'' and published by the President in April, 2011; and

(F) include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified information and other sensitive national security information.

(3) SUBMISSION.—The Attorney General shall submit to Congress—

(A) not later than 90 days after the date of the enactment of this Act, interim guidelines required under paragraph (1); and

(B) not later than 180 days after such date, final guidelines required under such paragraph.

(c) NATIONAL CYBER THREAT INTELLIGENCE INTEGRATION CENTER.—

(1) ESTABLISHMENT.—Title I of the National Security Act of 1947 (50 U.S.C. 3021 et seq.), as amended by section 2 of this Act, is further amended—

(A) by redesignating section 119B as section 119C; and

(B) by inserting after section 119A the following new section:

''SEC. 119B. CYBER THREAT INTELLIGENCE INTEGRATION CENTER.

''(a) ESTABLISHMENT.—There is within the Office of the Director of National Intelligence a Cyber Threat Intelligence Integration Center.

''(b) DIRECTOR.—There is a Director of the Cyber Threat Intelligence Integration Center, who shall be the head of the Cyber Threat Intelligence Integration Center, and who shall be appointed by the Director of National Intelligence.

''(c) PRIMARY MISSIONS.—The Cyber Threat Intelligence Integration Center shall—

''(1) serve as the primary organization within the Federal Government for analyzing and integrating all intelligence possessed or acquired by the United States pertaining to cyber threats;

''(2) ensure that appropriate departments and agencies have full access to and receive all-source intelligence support needed to execute the cyber threat intelligence activities of such agencies and to perform independent, alternative analyses;

''(3) disseminate cyber threat analysis to the President, the appropriate departments and agencies of the Federal Government, and the appropriate committees of Congress;

''(4) coordinate cyber threat intelligence activities of the departments and agencies of the Federal Government; and

''(5) conduct strategic cyber threat intelligence planning for the Federal Government.

''(d) LIMITATIONS.—The Cyber Threat Intelligence Integration Center shall—

''(1) have not more than 50 permanent positions;

''(2) in carrying out the primary missions of the Center described in subsection (c), may not augment staffing through detailees, assignees, or core contractor personnel or enter into any personal services contracts to exceed the limitation under paragraph (1); and

''(3) be located in a building owned or operated by an element of the intelligence community as of the date of the enactment of this section.''.

(2) TABLE OF CONTENTS AMENDMENTS.—The table of contents in the first section of the National Security Act of 1947, as amended by section 2 of this Act, is further amended by striking the item relating to section 119B and inserting the following new items:

''Sec. 119B. Cyber Threat Intelligence Integration Center.

''Sec. 119C. National intelligence centers.''.

(d) INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.—

(1) NO WAIVER OF PRIVILEGE OR PROTECTION.—The provision of a cyber threat indicator or defensive measure to the Federal Government under this Act shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

(2) PROPRIETARY INFORMATION.—Consistent with section 3(c)(2), a cyber threat indicator or defensive measure provided by a non-Federal entity to the Federal Government under this Act shall be considered the commercial, financial, and proprietary information of the non-Federal entity that is the originator of such cyber threat indicator or defensive measure when so designated by such non-Federal entity or a non-Federal entity acting in accordance with the written authorization of the non-Federal entity that is the originator of such cyber threat indicator or defensive measure.

(3) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator or defensive measure provided to the Federal Government under this Act shall be—

(A) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records; and

(B) withheld, without discretion, from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local provision of law requiring disclosure of information or records, except as otherwise required by applicable Federal, State, tribal, or local law requiring disclosure in any criminal prosecution.

(4) EX PARTE COMMUNICATIONS.—The provision of a cyber threat indicator or defensive measure to the Federal Government under this Act shall not be subject to a rule of any Federal department or agency or any judicial doctrine regarding ex parte communications with a decision-making official.

(5) DISCLOSURE, RETENTION, AND USE.—

(A) AUTHORIZED ACTIVITIES.—A cyber threat indicator or defensive measure provided to the Federal Government under this Act may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any department, agency, component, officer, employee, or agent of the Federal Government solely for—

(i) a cybersecurity purpose;

(ii) the purpose of responding to, prosecuting, or otherwise preventing or mitigating a threat of death or serious bodily harm or an offense arising out of such a threat;

(iii) the purpose of responding to, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(iv) the purpose of preventing, investigating, disrupting, or prosecuting any of the offenses listed in sections 1028, 1029, 1030, and 3559(c)(2)(F) and chapters 37 and 90 of title 18, United States Code.

(B) PROHIBITED ACTIVITIES.—A cyber threat indicator or defensive measure provided to the Federal Government under this Act shall not be disclosed to, retained by, or used by any Federal department or agency for any use not permitted under subparagraph (A).

(C) PRIVACY AND CIVIL LIBERTIES.—A cyber threat indicator or defensive measure provided to the Federal Government under this Act shall be retained, used, and disseminated by the Federal Government in accordance with—

(i) the policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government required by subsection (b) of section 111 of the National Security Act of 1947, as added by subsection (a) of this section; and

(ii) the privacy and civil liberties guidelines required by subsection (b).

SEC. 5. FEDERAL GOVERNMENT LIABILITY FOR VIOLATIONS OF PRIVACY OR CIVIL LIBERTIES.

(a) IN GENERAL.—If a department or agency of the Federal Government intentionally or willfully violates the privacy and civil liberties guidelines issued by the Attorney General under section 4(b), the United States shall be liable to a person injured by such violation in an amount equal to the sum of—

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

(2) reasonable attorney fees as determined by the court and other litigation costs reasonably incurred in any case under this subsection in which the complainant has substantially prevailed.

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

(1) the district in which the complainant resides;

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

(3) the district in which the department or agency of the Federal Government that violated such privacy and civil liberties guidelines is located; or

(4) the District of Columbia.

(c) 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 the privacy and civil liberties guidelines issued by the Attorney General under section 4(b) that is the basis for the action.

(d) 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 by a department or agency of the Federal Government under this Act.

SEC. 6. PROTECTION FROM LIABILITY.

(a) MONITORING OF INFORMATION SYSTEMS.—No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of an information system and information under section 3(a) that is conducted in good faith in accordance with this Act and the amendments made by this Act.

(b) SHARING OR RECEIPT OF CYBER THREAT INDICATORS.—No cause of action shall lie or be maintained in any court against any non-Federal entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure under section 3(c), or a good faith failure to act based on such sharing or receipt, if such sharing or receipt is conducted in good faith in accordance with this Act and the amendments made by this Act.

(c) WILLFUL MISCONDUCT.—

(1) RULE OF CONSTRUCTION.—Nothing in this section shall be construed—

(A) to require dismissal of a cause of action against a non-Federal entity (including a private entity) that has engaged in willful misconduct in the course of conducting activities authorized by this Act or the amendments made by this Act; or

(B) to undermine or limit the availability of otherwise applicable common law or statutory defenses.

(2) PROOF OF WILLFUL MISCONDUCT.—In any action claiming that subsection (a) or (b) does not apply due to willful misconduct described in paragraph (1), the plaintiff shall have the burden of proving by clear and convincing evidence the willful misconduct by each non-Federal entity subject to such claim and that such willful misconduct proximately caused injury to the plaintiff.

(3) WILLFUL MISCONDUCT DEFINED.—In this subsection, the term ''willful misconduct'' means an act or omission that is taken—

(A) intentionally to achieve a wrongful purpose;

(B) knowingly without legal or factual justification; and

(C) in disregard of a known or obvious risk that is so great as to make it highly probable that the harm will outweigh the benefit.

SEC. 7. OVERSIGHT OF GOVERNMENT ACTIVITIES.

(a) BIENNIAL REPORT ON IMPLEMENTATION.—

(1) IN GENERAL.—Section 111 of the National Security Act of 1947, as added by section 2(a) and amended by section 4(a) of this Act, is further amended—

(A) by redesignating subsection (c) (as redesignated by such section 4(a)) as subsection (d); and

(B) by inserting after subsection (b) (as inserted by such section 4(a)) the following new subsection:

''(c) BIENNIAL REPORT ON IMPLEMENTATION.—

''(1) IN GENERAL.—Not less frequently than once every two years, the Director of National Intelligence, in consultation with the heads of the other appropriate Federal entities, shall submit to Congress a report concerning the implementation of this section and the Protecting Cyber Networks Act.

''(2) CONTENTS.—Each report submitted under paragraph (1) shall include the following:

''(A) An assessment of the sufficiency of the policies, procedures, and guidelines required by this section and section 4 of the Protecting Cyber Networks Act in ensuring that cyber threat indicators are shared effectively and responsibly within the Federal Government.

''(B) An assessment of whether the procedures developed under section 3 of such Act comply with the goals described in subparagraphs (A), (B), and (C) of subsection (a)(1).

''(C) An assessment of whether cyber threat indicators have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purposes of this section and such Act.

''(D) A review of the type of cyber threat indicators shared with the Federal Government under this section and such Act, including the following:

''(i) The degree to which such information may impact the privacy and civil liberties of specific persons.

''(ii) A quantitative and qualitative assessment of the impact of the sharing of such cyber threat indicators with the Federal Government on privacy and civil liberties of specific persons.

''(iii) The adequacy of any steps taken by the Federal Government to reduce such impact.

''(E) A review of actions taken by the Federal Government based on cyber threat indicators shared with the Federal Government under this

section or such Act, including the appropriateness of any subsequent use or dissemination of such cyber threat indicators by a Federal entity under this section or section 4 of such Act.

''(F) A description of any significant violations of the requirements of this section or such Act by the Federal Government—

''(i) an assessment of all reports of officers, employees, and agents of the Federal Government misusing information provided to the Federal Government under the Protecting Cyber Networks Act or this section, without regard to whether the misuse was knowing or wilful; and

''(ii) an assessment of all disciplinary actions taken against such officers, employees, and agents.

''(G) A summary of the number and type of non-Federal entities that received classified cyber threat indicators from the Federal Government under this section or such Act and an evaluation of the risks and benefits of sharing such cyber threat indicators.

''(H) An assessment of any personal information of or information identifying a specific person not directly related to a cybersecurity threat that—

''(i) was shared by a non-Federal entity with the Federal Government under this Act in contravention of section 3(d)(2); or

''(ii) was shared within the Federal Government under this Act in contravention of the guidelines required by section 4(b).

''(3) RECOMMENDATIONS.—Each report submitted under paragraph (1) may include such recommendations as the heads of the appropriate Federal entities may have for improvements or modifications to the authorities and processes under this section or such Act.

''(4) FORM OF REPORT.—Each report required by paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

''(5) PUBLIC AVAILABILITY OF REPORTS.—The Director of National Intelligence shall make publicly available the unclassified portion of each report required by paragraph (1).''.

(2) INITIAL REPORT.—The first report required under subsection (c) of section 111 of the National Security Act of 1947, as inserted by paragraph (1) of this subsection, shall be submitted not later than one year after the date of the enactment of this Act.

(b) REPORTS ON PRIVACY AND CIVIL LIBERTIES.—

(1) BIENNIAL REPORT FROM PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD.—

(A) IN GENERAL.—Section 1061(e) of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee(e)) is amended by adding at the end the following new paragraph:

''(3) BIENNIAL REPORT ON CERTAIN CYBER ACTIVITIES.—

''(A) REPORT REQUIRED.—The Privacy and Civil Liberties Oversight Board shall biennially submit to Congress and the President a report containing—

''(i) an assessment of the privacy and civil liberties impact of the activities carried out under the Protecting Cyber Networks Act and the amendments made by such Act; and

''(ii) an assessment of the sufficiency of the policies, procedures, and guidelines established pursuant to section 4 of the Protecting Cyber Networks Act and the amendments made by such section 4 in addressing privacy and civil liberties concerns.

''(B) RECOMMENDATIONS.—Each report submitted under this paragraph may include such recommendations as the Privacy and Civil Liberties Oversight Board may have for improvements or modifications to the authorities under the Protecting Cyber Networks Act or the amendments made by such Act.

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

''(D) PUBLIC AVAILABILITY OF REPORTS.—The Privacy and Civil Liberties Oversight Board shall make publicly available the unclassified portion of each report required by subparagraph (A).''.

(B) INITIAL REPORT.—The first report required under paragraph (3) of section 1061(e) of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee(e)), as added by subparagraph (A) of this paragraph, shall be submitted not later than 2 years after the date of the enactment of this Act.

(2) BIENNIAL REPORT OF INSPECTORS GENERAL.—

(A) IN GENERAL.—Not later than 2 years after the date of the enactment of this Act and not less frequently than once every 2 years thereafter, the Inspector General of the Department of Homeland Security, the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, and the Inspector General of the Department of Defense, in consultation with the Council of Inspectors General on Financial Oversight, shall jointly submit to Congress a report on the receipt, use, and dissemination of cyber threat indicators and defensive measures that have been shared with Federal entities under this Act and the amendments made by this Act.

(B) CONTENTS.—Each report submitted under subparagraph (A) shall include the following:

(i) A review of the types of cyber threat indicators shared with Federal entities.

(ii) A review of the actions taken by Federal entities as a result of the receipt of such cyber threat indicators.

(iii) A list of Federal entities receiving such cyber threat indicators.

(iv) A review of the sharing of such cyber threat indicators among Federal entities to identify inappropriate barriers to sharing information.

(C) RECOMMENDATIONS.—Each report submitted under this paragraph may include such recommendations as the Inspectors General referred to in subparagraph (A) may have for improvements or modifications to the authorities under this Act or the amendments made by this Act.

(D) FORM.—Each report required under this paragraph shall be submitted in unclassified form, but may include a classified annex.

(E) PUBLIC AVAILABILITY OF REPORTS.—The Inspector General of the Department of Homeland Security, the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, and the Inspector General of the Department of Defense shall make publicly available the unclassified portion of each report required under subparagraph (A).

SEC. 8. REPORT ON CYBERSECURITY THREATS.

(a) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of other appropriate elements of the intelligence community, shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on cybersecurity threats, including cyber attacks, theft, and data breaches.

(b) CONTENTS.—The report required by subsection (a) shall include the following:

(1) An assessment of—

(A) the current intelligence sharing and cooperation relationships of the United States with other countries regarding cybersecurity threats (including cyber attacks, theft, and data breaches) directed against the United States that threaten the United States national security interests, economy, and intellectual property; and

(B) the relative utility of such relationships, which elements of the intelligence community participate in such relationships, and whether and how such relationships could be improved.

(2) A list and an assessment of the countries and non-state actors that are the primary threats of carrying out a cybersecurity threat (including a cyber attack, theft, or data breach) against the United States and that threaten the United States national security, economy, and intellectual property.

(3) A description of the extent to which the capabilities of the United States Government to respond to or prevent cybersecurity threats (including cyber attacks, theft, or data breaches) directed against the United States private sector are degraded by a delay in the prompt notification by private entities of such threats or cyber attacks, theft, and breaches.

(4) An assessment of additional technologies or capabilities that would enhance the ability of the United States to prevent and to respond to cybersecurity threats (including cyber attacks, theft, and data breaches).

(5) An assessment of any technologies or practices utilized by the private sector that could be rapidly fielded to assist the intelligence community in preventing and responding to cybersecurity threats.

(c) FORM OF REPORT.—The report required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(d) PUBLIC AVAILABILITY OF REPORT.—The Director of National Intelligence shall make publicly available the unclassified portion of the report required by subsection (a).

(e) INTELLIGENCE COMMUNITY DEFINED.—In this section, the term ''intelligence community'' has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

SEC. 9. CONSTRUCTION AND PREEMPTION.

(a) PROHIBITION OF SURVEILLANCE.—Nothing in this Act or the amendments made by this Act shall be construed to authorize the Department of Defense or the National Security Agency or any other element of the intelligence community to target a person for surveillance.

(b) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this Act or the amendments made by this Act shall be construed to limit or prohibit—

(1) otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity, by a non-Federal entity to any other non-Federal entity or the Federal Government; or

(2) any otherwise lawful use of such disclosures by any entity of the Federal government, without regard to whether such otherwise lawful disclosures duplicate or replicate disclosures made under this Act.

(c) WHISTLE BLOWER PROTECTIONS.—Nothing in this Act or the amendments made by this Act shall be construed to prohibit or limit the disclosure of information protected under section 2302(b)(8) of title 5, United States Code (governing disclosures of illegality, waste, fraud, abuse, or public health or safety threats), section 7211 of title 5, United States Code (governing disclosures to Congress), section 1034 of title 10, United States Code (governing disclosure to Congress by members of the military), or any similar provision of Federal or State law..

(d) PROTECTION OF SOURCES AND METHODS.—Nothing in this Act or the amendments made by this Act shall be construed—

(1) as creating any immunity against, or otherwise affecting, any action brought by the Federal Government, or any department or agency thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, or use of classified information;

(2) to affect the conduct of authorized law enforcement or intelligence activities; or

(3) to modify the authority of the President or a department or agency of the Federal Government to protect and control the dissemination of classified information, intelligence sources and methods, and the national security of the United States.

(e) RELATIONSHIP TO OTHER LAWS.—Nothing in this Act or the amendments made by this Act shall be construed to affect any requirement under any other provision of law for a non-Federal entity to provide information to the Federal Government.

(f) INFORMATION SHARING RELATIONSHIPS.—Nothing in this Act or the amendments made by this Act shall be construed—

(1) to limit or modify an existing information-sharing relationship;

(2) to prohibit a new information-sharing relationship; or

(3) to require a new information-sharing relationship between any non-Federal entity and the Federal Government.

(g) PRESERVATION OF CONTRACTUAL OBLIGATIONS AND RIGHTS.—Nothing in this Act or the amendments made by this Act shall be construed—

(1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any non-Federal entities, or between any non-Federal entity and a Federal entity; or

(2) to abrogate trade secret or intellectual property rights of any non-Federal entity or Federal entity.

(h) ANTI-TASKING RESTRICTION.—Nothing in this Act or the amendments made by this Act shall be construed to permit the Federal Government—

(1) to require a non-Federal entity to provide information to the Federal Government;

(2) to condition the sharing of a cyber threat indicator with a non-Federal entity on such non-Federal entity's provision of a cyber threat indicator to the Federal Government; or

(3) to condition the award of any Federal grant, contract, or purchase on the provision of a cyber threat indicator to a Federal entity.

(i) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this Act or the amendments made by this Act shall be construed to subject any non-Federal entity to liability for choosing not to engage in a voluntary activiy authorized in this Act and the amendments made by this Act.

(j) USE AND RETENTION OF INFORMATION.—Nothing in this Act or the amendments made by this Act shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use any information shared under this Act or the amendments made by this Act for any use other than permitted in this Act or the amendments made by this Act.

(k) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This Act and the amendments made by this Act supersede any statute or other provision of law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this Act or the amendments made by this Act.

(2) STATE LAW ENFORCEMENT.—Nothing in this Act or the amendments made by this Act shall be construed to supersede any statute or other provision of law of a State or political subdivision of a State concerning the use of authorized law enforcement practices and procedures.

(l) REGULATORY AUTHORITY.—Nothing in this Act or the amendments made by this Act shall be construed—

(1) to authorize the promulgation of any regulations not specifically authorized by this Act or the amendments made by this Act;

(2) to establish any regulatory authority not specifically established under this Act or the amendments made by this Act; or

(3) to authorize regulatory actions that would duplicate or conflict with regulatory requirements, mandatory standards, or related processes under another provision of Federal law.

SEC. 10. CONFORMING AMENDMENTS.

Section 552(b) of title 5, United States Code, is amended—

(1) in paragraph (8), by striking ''or'' at the end;

(2) in paragraph (9), by striking ''wells.'' and inserting ''wells; or''; and

(3) by inserting after paragraph (9) the following:

''(10) information shared with or provided to the Federal Government pursuant to the Protecting Cyber Networks Act or the amendments made by such Act.''.

SEC. 11. DEFINITIONS.

In this Act:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(2) APPROPRIATE FEDERAL ENTITIES.—The term ''appropriate Federal entities'' means the following:

(A) The Department of Commerce.

(B) The Department of Defense.

(C) The Department of Energy.

(D) The Department of Homeland Security.

(E) The Department of Justice.

(F) The Department of the Treasury.

(G) The Office of the Director of National Intelligence.

(3) CYBERSECURITY PURPOSE.—The term ''cybersecurity purpose'' means the purpose of protecting (including through the use of a defensive measure) an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability or identifying the source of a cybersecurity threat.

(4) CYBERSECURITY THREAT.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term ''cybersecurity threat'' means an action, not protected by the first amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, confidentiality, integrity, or availability of an information system or information that is stored on, processed by, or transiting an information system.

(B) EXCLUSION.—The term ''cybersecurity threat'' does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(5) CYBER THREAT INDICATOR.—The term ''cyber threat indicator'' means information or a physical object that is necessary to describe or identify—

(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

(B) a method of defeating a security control or exploitation of a security vulnerability;

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(E) malicious cyber command and control;

(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat; or

(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law.

(6) DEFENSIVE MEASURE.—The term ''defensive measure'' means an action, device, procedure, technique, or other measure executed on an information system or information that is stored on, processed by, or transiting an information system that prevents or mitigates a known or suspected cybersecurity threat or security vulnerability.

(7) FEDERAL ENTITY.—The term ''Federal entity'' means a department or agency of the United States or any component of such department or agency.

(8) INFORMATION SYSTEM.—The term ''information system''—

(A) has the meaning given the term in section 3502 of title 44, United States Code; and

(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

(9) LOCAL GOVERNMENT.—The term ''local government'' means any borough, city, county, parish, town, township, village, or other political subdivision of a State.

(10) MALICIOUS CYBER COMMAND AND CONTROL.—The term ''malicious cyber command and control'' means a method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

(11) MALICIOUS RECONNAISSANCE.—The term ''malicious reconnaissance'' means a method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(12) MONITOR.—The term ''monitor'' means to acquire, identify, scan, or otherwise possess information that is stored on, processed by, or transiting an information system.

(13) NON-FEDERAL ENTITY.—

(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term ''non-Federal entity'' means any private entity, non-Federal government department or agency, or State, tribal, or local government (including a political subdivision, department, officer, employee, or agent thereof).

(B) INCLUSIONS.—The term ''non-Federal entity'' includes a government department or agency (including an officer, employee, or agent thereof) of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(C) EXCLUSION.—The term ''non-Federal entity'' does not include a foreign power or known agent of a foreign power, as both terms are defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(14) PRIVATE ENTITY.—

(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term ''private entity'' means any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof.

(B) INCLUSION.—The term ''private entity'' includes a component of a State, tribal, or local government performing electric utility services.

(C) EXCLUSION.—The term ''private entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(15) REAL TIME; REAL-TIME.—The terms ''real time'' and ''real-time'' mean a process by which an automated, machine-to-machine system processes cyber threat indicators such that the time in which the occurrence of an event and the reporting or recording of it are as simultaneous as technologically and operationally practicable.

(16) SECURITY CONTROL.—The term ''security control'' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely impact the security, confidentiality, integrity, and availability of an information system or its information.

(17) SECURITY VULNERABILITY.—The term ''security vulnerability'' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

(18) TRIBAL.—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

The Acting CHAIR. No amendment to the committee amendment in the nature of a substitute shall be in order except those printed in part A of House

Report 114–88. Each such amendment may be offered only in the order printed in the report, by a Member designated in the report, shall be considered 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.

□ 1515

AMENDMENT NO. 1 OFFERED BY MR. NUNES

The Acting CHAIR. It is now in order to consider amendment No. 1 printed in part A of House Report 114–88.

Mr. NUNES. 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 5, beginning line 16, strike ''in accordance with'' and insert ''under''.

Page 9, line 2, strike ''and is limited to''.

Page 9, beginning line 14, strike ''the intentional or reckless operation of any'' and insert ''a''.

Page 9, beginning line 17, strike ''substantially harms, or initiates a new action, process, or procedure on'' and insert '', or substantially harms''.

Page 12, beginning line 2, strike ''a non-Federal entity, if authorized by applicable law or regulation other than this Act, from sharing'' and insert ''otherwise lawful sharing by a non-Federal entity of''.

Page 14, line 18, insert ''or defensive measure'' before ''shared''.

Page 23, line 19, strike ''section 3(c)(2)'' and insert ''this Act''.

Page 24, line 15, strike ''section 552(b)(3)(B)'' and insert ''section 552(b)(3)''.

Page 25, line 13, insert ''investigating,'' after ''to,''.

Page 25, line 18, insert ''investigating, prosecuting,'' after ''to,''.

Page 27, line 23, strike ''subsection'' and insert ''section''.

Page 27, beginning line 24, strike ''of the violation'' and all that follows through the period on page 28, line 2, and insert the following: ''on which the cause of action arises.''.

Page 28, line 4, strike ''subsection'' and insert ''section''.

Page 28, line 14, strike ''in good faith''.

Page 28, beginning line 22, strike ''in good faith''.

Page 33, line 16, insert ''of such Act'' before the semicolon.

Page 33, line 19, insert ''of such Act'' before the period.

Page 38, line 20, strike ''threats,'' and insert the following: ''threats to the national security and economy of the United States,''.

Page 44, line 2, strike ''activiy'' and insert ''activity''.

Page 44, after line 23, insert the following:

(3) STATE REGULATION OF UTILITIES.—Except as provided by section 3(d)(4)(B), nothing in this Act or the amendments made by this Act shall be construed to supersede any statute, regulation, or other provision of law of a State or political subdivision of a State relating to the regulation of a private entity performing utility services, except to the extent such statute, regulation, or other provision of law restricts activity authorized under this Act or the amendments made by this Act.

Strike section 10.

Page 51, line 13, strike ''electric''.

The Acting CHAIR. Pursuant to House Resolution 212, the gentleman from California (Mr. NUNES) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from California.

Mr. NUNES. Madam Chair, I offer this amendment to make certain technical changes to the bill. These changes will align several sections of the bill, including the authorization for the use of defensive measures and the liability protections, with the Committee on Homeland Security's bill, H.R. 1731.

The amendment also removes a direct amendment to the Freedom of Information Act because the bill already contains a strong exemption of cyber threat information and defensive measures from disclosure. The change does not have a substantive effect on the exemption of cyber threat information from disclosure laws.

The changes also reflect feedback we have received from our minority, from the executive branch, from outside groups, and from other committees of Congress. We want to make sure that the bill establishes a workable system for companies and the government to share cyber threat information and defensive measures.

I urge Members to support this technical and clarifying amendment, and I reserve the balance of my time.

Mr. SCHIFF. Madam Chair, I claim the time in opposition, although I am not opposed to the gentleman's amendment.

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

There was no objection.

Mr. SCHIFF. Madam Chair, the manager's amendment makes mostly technical edits to the bill which advanced out of the Intelligence Committee unanimously. These strong edits came from our close and continuing consultations with outside groups and with the White House.

There is still work that remains to be done. In particular, we are going to work, as the bill moves forward, on the liability section. In order to benefit from the liability protection under the current language, it is necessary for companies to strictly comply with the act, which means sharing information only for a cybersecurity purpose and taking reasonable efforts to remove private information before sharing it.

I would support making further changes to the bill to make this requirement even more clear. In particular, I think it would be advantageous to strike what is, in my view, an unnecessary section on the rule of construction pertaining to willful misconduct.

Striking the rule of construction will help further clarify the intent of the bill, which is that liability protection is only available if a company or other non-Federal entity shares cyber threat information, for a cybersecurity purpose, and only after it takes reasonable steps to remove private information not directly related to the cybersecurity threat.

That is the intention of the bill, and I think striking that section will make it more clear. If a company acts unreasonably—let alone recklessly or willfully—in following these requirements, it does not get liability protection, nor should it.

That is the right result, and we have to be careful not to create any confusion about there being any immunity for people or for companies acting willfully, recklessly, or even unreasonably in disregarding private information or the requirement that it be extricated.

The manager's amendment makes positive technical changes. There are further changes that I would like to see as the bill moves forward. Confusion in any section of the bill, particularly as it pertains to liability, means litigation, and litigation means costs, so I think there is further work for us to do to make it even more clear.

In sum, I support the technical and substantive changes made in the manager's amendment, and I urge my colleagues to do the same. I join the chairman in urging support for the manager's amendment.

I yield back the balance of my time.

Mr. NUNES. Madam Chair, as I have no other speakers, I urge my colleagues to support this amendment.

I yield back the balance of my time.

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

The amendment was agreed to.

AMENDMENT NO. 2 OFFERED BY MR. CÁRDENAS

The Acting CHAIR. It is now in order to consider amendment No. 2 printed in part A of House Report 114–88.

Mr. CÁRDENAS. Madam Chair, I am here to present my amendment.

The Acting CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 15, after line 7, insert the following:

(f) SMALL BUSINESS PARTICIPATION.—

(1) ASSISTANCE.—The Administrator of the Small Business Administration shall provide assistance to small businesses and small financial institutions to monitor information and information systems, operate defensive measures, and share and receive cyber threat indicators and defensive measures under this section

(2) REPORT.—Not later than one year after the date of the enactment of this Act, the Administrator of the Small Business Administration shall submit to the President a report on the degree to which small businesses and small financial institutions are able to engage in cyber threat information sharing under this section. Such report shall include the recommendations of the Administrator for improving the ability of such businesses and institutions to engage in cyber threat information sharing and to use shared information to defend their networks.

(3) OUTREACH.—The Federal Government shall conduct outreach to small businesses and small financial institutions to encourage such businesses and institutions to exercise their authority under this section.

The Acting CHAIR. Pursuant to House Resolution 212, the gentleman

from California (Mr. CÁRDENAS) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from California.

Mr. CÁRDENAS. Madam Chair, I rise today to speak in support of my amendment to H.R. 1560.

I applaud the managers of this legislation for all of their hard work. I understand the difficult balance that must be struck in this important debate, and I thank the committee for the opportunity to have my amendment considered today.

Madam Chair, this amendment will protect national security by starting from the ground up in protecting our smallest of businesses.

Cyber attacks are a real threat to our economy and national security. Hackers will look for the most vulnerable in the supply chain to exploit their security. This is why we must make sure any legislation related to cybersecurity places small businesses at the forefront of our security planning.

By doing this, we will be protecting customers and businesses up and down the supply chain, which will defend our economy, as a whole, from being attacked.

The amendment will ensure that the SBA will assist small businesses and small financial institutions in participating in the programs under this bill, and it will make sure the Federal Government performs outreach to small businesses and to small financial institutions.

This is a commonsense provision that addresses the issues that are critical to ensuring the security of our cyberspace and of our economic well-being now and into the future.

Small businesses are increasingly becoming the target of cyber criminals as larger companies increase their protections, so we need to arm them with the information and technical assistance they need to create effective plans to thwart these attacks and intrusions.

On a personal note, I once owned a small business myself. I left my bigger, corporate job to start a small business in my local community and employ people I grew up with. Washington is a faraway place for many small businesses in our country. The laws here can seem disconnected. The issues can be brushed off as someone else's problem.

That is why it is essential that, today and moving forward on all of these cybersecurity debates, that we make sure we have programs in place to work with and to educate our small businesses and that we understand that, every time one of these small businesses is successfully attacked and breached, it is a possibility that it could go under, losing those local jobs. I think this is a commonsense amendment.

I reserve the balance of my time.

Mr. NUNES. Madam Chair, I claim the time in opposition, although I am not opposed to the amendment.

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

There was no objection.

Mr. NUNES. Madam Chair, I want to thank the gentleman from California for bringing forward this thoughtful amendment. He worked closely with the committee to ensure that the language did not disrupt the intent of the bill. I am prepared to accept the amendment.

I yield back the balance of my time.

Mr. CÁRDENAS. Madam Chair, I yield the balance of my time to the gentleman from California (Mr. SCHIFF).

Mr. SCHIFF. I thank the gentleman, my colleague, for yielding.

Madam Chair, for a large business, a cyber attack can be costly and damaging. For a small business, a cyber attack can be fatal, wiping out a family's dream or a lifetime of work in a few clicks of a mouse.

Small businesses and small financial institutions also don't have the large legal shops that are sometimes necessary to keep up with the latest changes or regulations coming from Washington.

That is why I am so pleased that my California colleague offered this important amendment. While I don't expect that any sharing mechanism will ultimately be costly to maintain or to access, there will be some costs, especially in the early stages of implementation, and there will be some new procedures to navigate.

This amendment will help put the reach and authority of the Small Business Administration in the service of cybersecurity by having the agency assist in the rollout of cyber threat information sharing.

It is an important addition to the bill. I thank the gentleman for raising the issue, and I urge my colleagues to support it.

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

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

The amendment was agreed to.

AMENDMENT NO. 3 OFFERED BY MR. CARSON OF INDIANA

The Acting CHAIR. It is now in order to consider amendment No. 3 printed in part A of House Report 114–88.

Mr. CARSON of Indiana. 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 37, after line 16, insert the following new clause:

(v) A review of the current procedures pertaining to the sharing of information, removal procedures for personal information or information identifying a specific person, and any incidents pertaining to the improper treatment of such information.

The Acting CHAIR. Pursuant to House Resolution 212, the gentleman from Indiana (Mr. CARSON) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentleman from Indiana.

Mr. CARSON of Indiana. Madam Chair, I proudly supported this bill when we marked it in the Intelligence Committee. I am only bringing up this amendment today to address a basic transparency concern raised by my constituents after the markup, that the cybersecurity threat posed to our government, to our businesses, and to our personal information is massive and is growing every day.

This bill provides important tools to ensure that the lessons learned from a breach of one company can help strengthen the security of others. As a result, your Social Security and credit card numbers will be better protected.

Madam Chair, as someone who opposed CISPA last year, I feel like this iteration is a major first step forward in privacy protection and transparency. I am particularly happy with the robust protections of personally identifiable information.

Unlike past iterations, this bill mandates that cyber threat information is scanned and that personal information is removed not once, but twice, before it can be transmitted to other Federal agencies.

I am pleased, Madam Chair, that companies will share their cyber threat information with a civilian agency and not directly with the intelligence community. I am also happy that additional limitations are placed on the ways that cyber threat information can be utilized.

For all of the benefits of this bill, the American people still—rightfully so—expect oversight that is consistent and comprehensive. That is what this amendment is all about. It strengthens the oversight of the inspector general's monitoring of this kind of information sharing.

Now, with this amendment, the inspector general will oversee and report on the process for information-sharing procedures, for removing personal information, and any incidence in which this information was treated improperly.

It will ensure Congress and the public that sharing is happening properly and that the public is being protected. I hope that my good Republican colleagues will support this amendment.

I reserve the balance of my time.

Mr. NUNES. Madam Chair, I claim the time in opposition, although I am not opposed to the amendment.

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

There was no objection.

Mr. NUNES. Madam Chair, I want to thank the gentleman. He is a member of the Intelligence Committee and has played a very productive and constructive role. As he said, his constituents have brought these concerns to him. He worked with the ranking member and

me, and we are prepared to accept the amendment.

I yield back the balance of my time.

□ 1530

Mr. CARSON of Indiana. Madam Chair, I yield 2 minutes to the gentleman from California (Mr. SCHIFF), my good friend.

Mr. SCHIFF. I thank the gentleman for yielding.

Madam Chair, this is Mr. CARSON's first year on the committee, and I appreciate his dedicated service and the interest he has taken in oversight of the intelligence community. He brings a background in law enforcement, which is a very welcome addition to our committee, and joins other colleagues with a very similar background.

He has worked closely with us to make privacy improvements throughout the process. I support his efforts here again to make a good bill even better. Mr. CARSON's amendment would include a requirement to make sure the critical dual privacy scrub is working the way it should. This is very important. It is at the core of our bill and at the core of our efforts to protect privacy. So we must monitor how these requirements are working and support transparent reporting to make sure that they are working as intended.

I support the amendment and urge my colleagues to do the same.

Mr. CARSON of Indiana. I thank Chairman NUNES and Ranking Member SCHIFF once again for their support in helping to keep our communities safer, but I still want to thank my Republican colleagues for supporting this amendment, and I thank them for their friendship. As a new member of the committee, Madam Chair, I have greatly appreciated the guidance—bipartisan guidance, if you will.

Every Member of this House, Madam Chair, has heard from constituents who are concerned about government surveillance and overreach. After everything we have heard about bulk collection over the last few years, the American people are right to be concerned about new authorities to collect data.

As the text plainly and repeatedly states, this is not a surveillance bill. We have protections in place to ensure that the intelligence community cannot collect and utilize your personal data. This amendment simply ensures that Congress and the public get to see this sharing process and see how it works if these protections happen to fail. I urge support for this amendment and the underlying bill.

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

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

The amendment was agreed to.

AMENDMENT NO. 4 OFFERED BY MR. MULVANEY

The Acting CHAIR. It is now in order to consider amendment No. 4 printed in part A of House Report 114–88.

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:

Add at the end the following new section:

SEC. 12. SUNSET.

This Act and the amendments made by this Act shall terminate on the date that is seven years after the date of the enactment of this Act.

The Acting CHAIR. Pursuant to House Resolution 212, 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. Madam Chair, I thank the chairman of the committee for the opportunity to present the amendment here today.

Very briefly, I will talk about the genesis of this amendment, which is very simple, by the way. It adds a 7-year sunset to all the provisions of the bill.

Madam Chair, in going through the review of this bill, it occurred to me that this was a really close call. There were folks whom I respect with a great deal of credibility who reached out to me and said: Look, here are the difficulties with this bill and why we should defeat this bill. At the same time, there are a lot of folks for whom I have a great deal of respect and have a great deal of credibility in the industry who also reached out to me and said: Look, this is a very serious problem. Here are the good things in the bill, and here is why you should support it.

It is probably not unusual that we have that circumstance before us where it is a close call. We are balancing two very critical things: security—specifically, cybersecurity—on one hand, and privacy, liberty interests, on the other. It is a balancing act that we are called on to do many, many times here in Washington, D.C.

As I was going through the bill, taking input from both sides of the argument, it occurred to me: All right, what if we have got it wrong? What if we have the balancing act wrong? Sure, we can go back in and fix it at some point in the future, some indeterminate time in the future; but face it, this is a busy place, with a lot of bills demanding attention on any given day in Congress.

Wouldn't it be nice to have something hardwired into the bill that would force Congress at some point in the future to come back and say: Okay. A couple years back, here is what we did on cybersecurity. Is it working? Did we get it right? Is the balance between security and privacy one that is serving both of those very important interests correctly?

We sat down to talk amongst some of my colleagues about the amount of time that was necessary. Madam Chair, 7 years is a long time to have a sunset provision in a bill. It came to my attention, though, given the complexities, the complexities of the systems necessary to be put in place in order to implement the programs in the bill, that 7 years was the appropriate level of time.

I am glad that we have sunset provisions in other pieces of legislation. I doubt very seriously we would be having serious discussions right now about things as important as the PATRIOT Act if a sunset provision was not hardwired into the bill. Maybe we should consider adding these to every single piece of legislation for just the same reason: to force us from time to time to see if what we thought we were doing several years ago was really as good an idea as we thought it was several years ago. So that was the intention.

That is the genesis of this amendment—again, very simple, a 7-year sunset provision. I hope my colleagues will see fit to support it.

I reserve the balance of my time.

Mr. NUNES. Madam Chair, I rise in opposition to this amendment, although I appreciate my colleague's concern.

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

Mr. NUNES. Madam Chair, my friend from South Carolina, I think, is very thoughtful in his approach in wanting sunset provisions in many laws that pass this body, and I think that is correct on major pieces of legislation, especially involving government bureaucracies, the creation of government bureaucracies, and the implementation of regulation.

I would just make a few important points that I think this bill is very different because this is a voluntary bill. It is also legislation that, because of the liability protections that are in this bill, if you have a sunset clause in it—and part of the reason why the other amendments that were made out of order and this one was made in order, because it was the longest time, with the 7 years, as the gentleman said—it is tough for a company to design, build, get in the process of preparing how they are going to share this information company to company, and I am afraid that even though this is 7 years, will companies make the investment terms of being willing to actually share? Then, if this expires, what happens with the trial lawyers that would then come after the fact when the Congress doesn't act with information that is sitting out there that no longer has the protections?

This is actually why, back when the last version of this legislation was up last Congress, we made several changes since then, and we have many more supporters since that time because of the changes we have made to make sure that we have scrubbed private data, to make sure this doesn't go to any government agency, to make sure that it is voluntary, all of the steps that we have taken. But because of the trial lawyer component and the liability being left open, this is why groups

like Heritage, in the last Congress, opposed an amendment just like this.

We would like to work with the gentleman and his colleagues on this, but I would ask if he would be willing to maybe work with us in a potential conference or possibly down the road, if it might be appropriate. I hate to oppose this amendment because he is my good friend, but I want to try to see if he might be willing to withdraw and work with us when we get to a conference on a reasonable solution to this.

I reserve the balance of my time.

Mr. MULVANEY. I will respond in a couple of different ways.

Under ordinary circumstances, Madam Chair, I might consider withdrawing the amendment, but I think we are here today under a somewhat extraordinary rule. I do appreciate the chairman's genuineness in his request because we have worked very closely together on other matters in the past. I look forward to working with him on other matters in the future. I consider him to be a good friend and colleague. But because of the nature of the joint rule, if this bill passes and the bill that is being offered by the Homeland Security Committee tomorrow passes as well, my understanding is those two bills will then be merged. I have a similar amendment, Madam Chair, tomorrow to Mr. MCCAUL's bill, so I am not really sure if even withdrawing at this point would accomplish the necessary end that you seek. I will politely decline your request, and respectfully so.

I will point out, my good friend does mention an interesting part of my history here in Washington, D.C. When I offered a similar amendment to, I believe, the PATRIOT Act a couple years back, The Heritage Foundation did oppose it. It always makes me smile, Madam Chair, when I remember going through that conversation with my friends over at The Heritage Foundation, and I had to send them a copy of Ed Feulner's own book. Ed, of course, is one of the founding members of The Heritage Foundation, and the last chapter is an exhortation to please include a sunset provision in every single piece of Federal legislation. Again, that just sort of makes me smile.

With all due respect due to the chairman, both as the chair of the committee and a Member of this body and a friend of mine, I will politely decline his request.

I yield back the balance of my time.

Mr. NUNES. I now yield 1 minute to the gentleman from Texas (Mr. FARENTHOLD).

Mr. FARENTHOLD. I appreciate the chairman yielding time to me, even though I am in support of this amendment.

Madam Chair, we need this legislation because our companies, our industries, our government, and even our individual citizens are under attack by foreign cyber hackers, under attack from criminals. We need the cooperation between the government and the private sector, but unfortunately we have seen that well-meaning folks in the government sometimes get a little overzealous in their data collection we don't always see.

For instance, section 215 of the PATRIOT Act, we saw in the Snowden revelations that every bit of metadata on phones was being collected. We didn't know that when we passed the PATRIOT Act. Now we have an opportunity to put a backstop in place where we can take a look a few years down the road and make sure this isn't being misinterpreted, not in line with congressional intent, and not in line with the Constitution. This backstop, this sunset, is a critical piece of the bill. The bill is not perfect, but this makes it a whole lot better and gives us a second bite at the apple should things be going wrong.

I appreciate your yielding.

Mr. NUNES. Madam Chair, I am prepared to close.

I would just say that I hate to have to oppose this amendment because I think my colleagues are offering it in good faith, with good intentions. However, it is a voluntary program. As I said, cybersecurity is going to continue to be an ever-increasing problem and challenge, and the last thing we want to do is put a backstop in to where companies or private citizens are afraid to share the information with each other because they are afraid of being sued by some trial lawyer down the road.

Like I said, I hate to oppose the amendment, but I will have to oppose the amendment and urge my colleagues to vote ''no.''

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 noes 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

The Acting CHAIR. It is now in order to consider amendment No. 5 printed in part A of House Report 114–88.

Ms. JACKSON LEE. 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:

Add at the end the following:

SEC. 12. COMPTROLLER GENERAL REPORT ON REMOVAL OF PERSONAL IDENTIFYING INFORMATION.

(a) REPORT.—Not later than three years after the date of the enactment of this Act, the Comptroller General of the United States shall submit to Congress a report on the actions taken by the Federal Government to remove personal information from cyber threat indicators pursuant to section 4(b).

(b) FORM.—The report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

The Acting CHAIR. Pursuant to House Resolution 212, the gentlewoman from Texas (Ms. JACKSON LEE) and a Member opposed each will control 5 minutes.

The Chair recognizes the gentlewoman from Texas.

□ 1545

Ms. JACKSON LEE. Madam Chair, I thank the manager and the chairman and ranking member of the House Intelligence Committee for their service and leadership.

I offer this amendment that I believe will answer a question that has been raised by many Members but really has bipartisan support.

This amendment is offered as a Jackson Lee-Polis amendment, and the specifics of it say:

''Not later than three years after the date of the enactment of this Act, the Comptroller General of the United States shall submit to Congress a report on the actions taken by the Federal Government to remove personal information from cyber threat indicators pursuant to section 4(b).''

Again, this relates to the concern that many of us will hear over and over again from our constituents.

In the world of hacking and mistakes and misdirection and unfairness and terrorism, it is important to secure this Nation and to be able to have the right information.

As I serve as a member of the Homeland Security Committee, I believe we have to have information to thwart terrorist acts and protect the homeland.

But there is a public benefit to my amendment. This amendment will provide the public assurance from a reliable and trustworthy source that their privacy and civil liberties are not being compromised.

We are a State and a Nation born out of the existence of the Bill of Rights. Along with the Constitution, it has framed a democracy, but it has also framed the preciousness of individual rights and privacy. I offer this amendment, again, to emphasize the importance of privacy that is so very important.

The Jackson Lee-Polis amendment provides, again, for a Government Accountability Act report to Congress on the actions taken by the Federal Government to remove personal information from data shared through the programs established by this statute.

The intent of the report, as indicated, is to provide Congress with information regarding the effectiveness of protecting the privacy of Americans.

Again, this amendment would result in the sole external report on the privacy and civil liberties impact of the programs created under this bill.

Privacy is of great concern to the American people. I know that because, as we were doing the Patriot Act in the

shadow of the heinous acts of 9/11, I will tell you that large voices were raised, particularly out of the Judiciary Committee and in working with the Intelligence Committee, about the issues of privacy. Americans understand that.

Privacy is of great concern to the American public. Privacy involves the handling and protection of personal information. And as well, when personal information is improperly accessed, used, or abused, it can cause financial and personal harm to those whose data is involved.

Madam Chair, may I ask how much time is remaining?

The Acting CHAIR. The gentlewoman from Texas has 2 minutes remaining.

Ms. JACKSON LEE. Madam Chair, I ask my colleagues to support the Jackson Lee amendment.

I yield 2 minutes to the gentleman from California (Mr. SCHIFF), the distinguished ranking member.

Mr. SCHIFF. Madam Chair, I thank the gentlewoman from Texas and the gentleman from Colorado for their amendment, and I am happy to support it.

We create a lot of law in this body, and it is absolutely necessary that we establish reporting mechanisms that allow us to measure the effectiveness of the work that we do here. This is an amendment that will do just that.

By requiring regular reports on the operation of the sharing mechanism that we are creating today, we can determine whether it is working as intended or whether it needs to be tweaked or changed to be more effective. We must always ensure that the government is fulfilling its obligation under this bill to remove personal information.

Again, I want to thank SHEILA JACKSON LEE, as well as the gentleman from Colorado, for their efforts. I support the amendment.

Ms. JACKSON LEE. Madam Chair, how much time is remaining?

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

Ms. JACKSON LEE. Thank you, Madam Chair.

Let me quickly say that a report on consumer views on the privacy issue published by the Pew Center found that a majority of adults surveyed felt that their privacy is being challenged along such core dimensions as the security of their personal information and their ability to retain confidentiality.

It is for this reason that I believe the Jackson Lee amendment, in conjunction with the underlying legislation, H.R. 1560, will be an added asset to ensure that the personal data, privacy, and civil liberties of Americans are protected.

Madam Chair, I offer my thanks to Chairman NUNES, and Ranking Member SCHIFF for their leadership and work on H.R. 1560.

The bipartisan work done by the House Select Committee on Intelligence resulted in H.R. 1560 being brought before the House for consideration.

I offer acknowledgement to Congressman POLIS in joining me in sponsoring this amendment.

The Jackson Lee-Polis Amendment to H.R. 1560 is simple and would improve the bill.

Jackson Lee Amendment designated #5 on the list of amendments approved for H.R. 1560:

The Jackson Lee-Polis Amendment provides for a Government Accountability Office (GAO) report to Congress on the actions taken by the Federal Government to remove personal information from data shared through the programs established by this statute.

The intent of the report is to provide Congress with information regarding the effectiveness of protecting the privacy of Americans.

This amendment would result in the sole external report on the privacy and civil liberties impact of the programs created under this bill.

Privacy is of great concern to the American public.

Privacy involves the handling and protection of personal information that individuals provide in the course of everyday commercial transactions.

When personal information is improperly accessed, used, or abused it can cause financial and personal harm to the people whose data is involved.

A report on consumer views on their privacy published by the Pew Center found that a majority of adults surveyed felt that their privacy is being challenged along such core dimensions as the security of their personal information and their ability to retain confidentiality.

For this reason, the Jackson Lee amendment providing an independent report to the public on how their privacy and civil liberties are treated under the implementation of this bill is important.

I ask that my colleagues on both sides of the aisle support this amendment.

I ask that the amendment be supported, and I yield back the balance of my time.

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

The amendment was agreed to.

AMENDMENT NO. 4 OFFERED BY MR. MULVANEY

The Acting CHAIR. Pursuant to clause 6 of rule XVIII, 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 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 313, noes 110, not voting 8, as follows:

[Roll No. 168]

AYES—313

Adams
Aguilar
Allen
Amash
Ashford
Babin
Barton
Bass
Beatty
Becerra
Bera
Beyer
Bilirakis
Bishop (GA)
Bishop (UT)
Black
Blum
Blumenauer
Bonamici
Bost
Boyle, Brendan F.
Brady (PA)
Brat
Bridenstine
Brooks (AL)
Brown (FL)
Brownley (CA)
Buchanan
Buck
Burgess
Bustos
Butterfield
Byrne
Capps
Capuano
Cárdenas
Carney
Carson (IN)
Carter (GA)
Cartwright
Castor (FL)
Castro (TX)
Chabot
Chaffetz
Chu, Judy
Cicilline
Clark (MA)
Clarke (NY)
Clawson (FL)
Clay
Cleaver
Clyburn
Cohen
Cole
Collins (GA)
Connolly
Conyers
Cooper
Costa
Courtney
Cramer
Crowley
Cummings
Davis (CA)
DeFazio
DeGette
Delaney
DeLauro
DelBene
Denham
DeSantis
DeSaulnier
DesJarlais
Deutch
Dingell
Doggett
Doyle, Michael F.
Duckworth
Duffy
Duncan (SC)
Duncan (TN)
Edwards
Ellison
Ellmers (NC)
Emmer (MN)
Engel
Eshoo
Esty
Farenthold
Farr
Fattah
Fitzpatrick
Fleischmann
Fleming
Flores
Forbes
Fortenberry
Foster
Foxx
Frankel (FL)
Franks (AZ)
Fudge
Gabbard
Gallego
Garamendi
Garrett
Gibbs
Gibson
Gohmert
Goodlatte
Gosar
Gowdy
Graham
Granger
Graves (GA)
Graves (LA)
Grayson
Green, Al
Green, Gene
Griffith
Grijalva
Grothman
Guinta
Gutiérrez
Hahn
Hanna
Harris
Heck (WA)
Hensarling
Herrera Beutler
Hice, Jody B.
Higgins
Himes
Hinojosa
Honda
Hoyer
Huelskamp
Huffman
Huizenga (MI)
Hultgren
Hunter
Hurt (VA)
Issa
Jackson Lee
Jeffries
Johnson (GA)
Johnson (OH)
Johnson, E. B.
Jolly
Jones
Jordan
Joyce
Kaptur
Keating
Kelly (IL)
Kennedy
Kildee
Kilmer
Kind
King (IA)
Kline
Kuster
Labrador
LaMalfa
Lamborn
Langevin
Larsen (WA)
Larson (CT)
Latta
Lawrence
Lee
Levin
Lewis
Lieu, Ted
Lipinski
Loebsack
Lofgren
Loudermilk
Love
Lowenthal
Lowey
Lucas
Luetkemeyer
Lujan Grisham (NM)
Luján, Ben Ray (NM)
Lummis
Lynch
Maloney, Sean
Marchant
Massie
Matsui
McClintock
McCollum
McDermott
McGovern
McMorris Rodgers
McNerney
Meadows
Meeks
Meng
Miller (FL)
Mooney (WV)
Moore
Moulton
Mullin
Mulvaney
Nadler
Napolitano
Neal
Neugebauer
Noem
Nolan
Norcross
Nugent
O'Rourke
Palazzo
Pallone
Palmer
Pascrell
Paulsen
Payne
Pearce
Pelosi
Perlmutter
Perry
Peters
Peterson
Pingree
Pitts
Pocan
Poe (TX)
Polis
Posey
Price (NC)
Price, Tom
Quigley
Rangel
Ribble
Rice (NY)
Rice (SC)
Richmond
Rigell
Roe (TN)
Rohrabacher
Rokita
Ross
Rothfus
Rouzer
Roybal-Allard
Ruiz
Rush
Russell
Salmon
Sánchez, Linda T.
Sanchez, Loretta
Sanford
Sarbanes
Scalise
Schakowsky
Schiff
Schrader
Schweikert
Scott (VA)
Scott, Austin
Scott, David
Serrano
Sessions
Sewell (AL)
Sherman
Sires
Slaughter
Smith (MO)
Smith (NE)
Smith (NJ)
Smith (TX)
Speier
Stefanik
Stutzman
Swalwell (CA)
Takai
Takano
Thompson (CA)
Thompson (MS)
Thompson (PA)
Tipton
Titus
Tonko
Torres
Tsongas
Van Hollen
Vargas
Veasey
Vela
Velázquez
Visclosky
Walker
Walorski
Walz
Waters, Maxine
Watson Coleman
Weber (TX)
Webster (FL)
Welch

Westerman	Wittman	Zeldin
Williams	Yarmuth	Zinke
Wilson (FL)	Yoder	
Wilson (SC)	Yoho	

NOES—110

Abraham	Hudson	Reichert
Aderholt	Hurd (TX)	Renacci
Amodei	Israel	Roby
Barletta	Jenkins (KS)	Rogers (AL)
Barr	Jenkins (WV)	Rogers (KY)
Benishek	Johnson, Sam	Rooney (FL)
Bishop (MI)	Katko	Ros-Lehtinen
Blackburn	Kelly (PA)	Roskam
Boustany	King (NY)	Royce
Brooks (IN)	Kinzinger (IL)	Ruppersberger
Bucshon	Kirkpatrick	Ryan (OH)
Calvert	Knight	Ryan (WI)
Carter (TX)	Lance	Sensenbrenner
Coffman	LoBiondo	Shimkus
Collins (NY)	Long	Shuster
Comstock	MacArthur	Simpson
Conaway	Maloney, Carolyn	Sinema
Cook	Marino	Stewart
Costello (PA)	McCarthy	Stivers
Crawford	McCaul	Thornberry
Crenshaw	McHenry	Tiberi
Cuellar	McKinley	Trott
Culberson	McSally	Turner
Davis, Danny	Meehan	Upton
Davis, Rodney	Messer	Valadao
Dent	Mica	Wagner
Diaz-Balart	Miller (MI)	Walberg
Dold	Moolenaar	Walden
Fincher	Murphy (PA)	Walters, Mimi
Frelinghuysen	Newhouse	Wenstrup
Guthrie	Nunes	Westmoreland
Hardy	Pittenger	Whitfield
Harper	Poliquin	Womack
Hartzler	Pompeo	Woodall
Heck (NV)	Ratcliffe	Young (AK)
Hill	Reed	Young (IA)
Holding		Young (IN)

NOT VOTING—8

Brady (TX)	Hastings	Smith (WA)
Curbelo (FL)	Murphy (FL)	Wasserman Schultz
Graves (MO)	Olson	

□ 1620

Messrs. ISRAEL, FINCHER, CALVERT, RYAN of Wisconsin, TURNER, SAM JOHNSON of Texas, Mrs. CAROLYN B. MALONEY of New York, Messrs. ABRAHAM, and RUPPERSBERGER changed their vote from ''aye'' to ''no.''

Ms. ADAMS, Mr. MILLER of Florida, Ms. PELOSI, Mses. EDWARDS, LORETTA SANCHEZ of California, Messrs. ROHRABACHER, CARNEY, ZELDIN, ROSS, RICHMOND, Mses. MATSUI, STEFANIK, Messrs. SIRES, CROWLEY, Mses. SCHAKOWSKY, DeGETTE, TITUS, Messrs. JOYCE, SEAN PATRICK MALONEY of New York, VEASEY, Mses. BROWNLEY of California, LEE, and Mr. PETERSON changed their vote from ''no'' to ''aye.''

So the amendment was agreed to.

The result of the vote was announced as above recorded.

The Acting CHAIR (Mr. THOMPSON of Pennsylvania). The question is on the committee 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. HULTGREN) having assumed the chair, Mr. THOMPSON of Pennsylvania, 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. 1560) to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes, and, pursuant to House Resolution 212, 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 committee 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

Miss RICE of New York. Mr. Speaker, I have a motion to recommit at the desk.

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

Miss RICE of New York. I am opposed to it in its current form.

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

The Clerk read as follows:

Miss Rice of New York moves to recommit the bill H.R. 1560 to the Select Committee on Intelligence (Permanent Select) with instructions to report the same back to the House forthwith, with the following amendment:

Page 22, line 14, strike ''and''.

Page 22, line 16, strike the period and insert a semicolon.

Page 22, after line 16, insert the following:

''(6) to prevent a terrorist attack against the United States, ensure that the appropriate departments and agencies of the Federal Government prioritize the sharing of cyber threat indicators regarding known terrorist organizations (including the Islamic State, al Qaeda, al Qaeda in the Arabian Peninsula, and Boko Haram) with respect to—

''(A) cyberattacks;

''(B) the recruitment of homegrown terrorists by such terrorist organizations; and

''(C) travel by persons to and from foreign countries in which such terrorist organizations are based or provide training (including Syria, Iraq, Yemen, Afghanistan, and Nigeria); and

''(7) to prevent the intelligence and military capability of the United States from being improperly transferred to any foreign country, terrorist organization, or state sponsor of terrorism, ensure that the appropriate departments and agencies of the Federal Government prioritize the sharing of cyber threat indicators regarding attempts to steal the military technology of the United States by state-sponsored computer hackers from the People's Republic of China and other foreign countries.''.

Mr. NUNES (during the reading). Mr. Speaker, I ask unanimous consent to dispense with the reading.

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

There was no objection.

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman is recognized for 5 minutes in support of her motion.

Miss RICE of New York. Mr. Speaker, this is the final amendment to the bill, which will not kill the bill or send it back to committee. If adopted, the bill will immediately proceed to final passage, as amended.

Mr. Speaker, the most important job we have is to protect the American homeland and the American people. The threats against our country are ceaseless and constantly evolving, and we too must evolve and adapt in our efforts to maintain the domestic security that the American people have entrusted us to uphold.

Passing H.R. 1560 will be a significant step forward in that effort. Our Nation's cyber infrastructure is under attack every single day from hackers, from foreign nations, and from terrorists. I believe H.R. 1560 will strengthen our government's ability to coordinate with companies in the private sector, share intelligence, and respond to these threats, but I also believe the legislation should be stronger.

We know that foreign nations and terrorist organizations are actively seeking to steal American military intelligence and technology, and we know that terrorists are using the Internet to spread their poisonous ideology, recruit American citizens to join their ranks, and encourage attacks here in America. Just this week, six Minnesota men were arrested after trying to travel to Syria to join the Islamic State. Last week, authorities arrested an Ohio man who actually trained with a terrorist group in Syria and returned to the U.S., intent on carrying out an attack on our soil. Earlier this month, two women in my home State of New York were arrested for planning to detonate a bomb in New York City.

Mr. Speaker, this amendment will help prevent a domestic terror attack by allowing Federal agencies to coordinate and prioritize the sharing of cyber threat intelligence regarding known terrorist organizations like the Islamic State, Boko Haram, al Shabaab, and al Qaeda and its affiliates, groups that use the Internet and social media as a weapon in their efforts to attack the United States and the American people. Likewise, this amendment will direct Federal agencies to prioritize the sharing of intelligence regarding attempts by terrorists and foreign nations to steal American military technology.

This amendment will help protect our Nation and the people we serve. I have no doubt that that is the highest priority for my colleagues on both sides of the aisle, so we must also make it a priority to neutralize these threats and do all that we can to thwart the violent ambitions of those who want to do us harm.

Again, Mr. Speaker, I believe H.R. 1560 is important legislation that deserves bipartisan support, but I believe this amendment deserves the same. It

will make the legislation stronger, make the American people safer, and I urge my colleagues on both sides of the aisle to give it their full support.

Mr. Speaker, I yield back the balance of my time.

Mr. NUNES. Mr. Speaker, I rise in opposition to the motion to recommit.

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

Mr. NUNES. Mr. Speaker, this motion to recommit is nothing more than a poison pill designed to destroy the years of work that have gone into crafting this legislation.

The bill already does exactly what the motion to recommit purposes. It helps the American people defend themselves against hackers from countries like China, Russia, Iran, North Korea, and other terrorist groups.

While we stand here and continue to debate this problem, our country is under attack from hackers who steal our intellectual property, pilfer our personal information, and target our national security interests.

I urge my colleagues to vote ''no'' on the motion to recommit and ''yes'' on final passage.

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.

RECORDED VOTE

Miss RICE of New York. Mr. Speaker, I demand a recorded vote.

A recorded vote was ordered.

The SPEAKER pro tempore. Pursuant to clause 9 of rule XX, this 5-minute vote on the motion to recommit will be followed by a 5-minute vote on the passage of the bill, if ordered.

The vote was taken by electronic device, and there were—ayes 183, noes 239, not voting 9, as follows:

[Roll No. 169]

AYES—183

Adams
Aguilar
Ashford
Bass
Beatty
Becerra
Bera
Beyer
Bishop (GA)
Blumenauer
Bonamici
Boyle, Brendan F.
Brady (PA)
Brown (FL)
Brownley (CA)
Bustos
Butterfield
Capps
Capuano
Cárdenas
Carney
Carson (IN)
Cartwright
Castor (FL)
Castro (TX)
Chu, Judy
Cicilline
Clark (MA)
Clarke (NY)
Clay
Cleaver
Clyburn
Cohen
Connolly
Conyers
Cooper
Costa
Courtney
Crowley
Cuellar
Cummings
Davis (CA)
Davis, Danny
DeFazio
DeGette
Delaney
DeLauro
DelBene
DeSaulnier
Deutch
Dingell
Doggett
Doyle, Michael F.
Duckworth
Edwards
Ellison
Engel
Eshoo
Esty
Farr
Fattah
Foster
Frankel (FL)
Fudge
Gabbard
Gallego
Garamendi
Graham
Grayson
Green, Al
Green, Gene
Grijalva
Gutiérrez
Hahn
Heck (WA)
Higgins
Himes
Hinojosa
Honda
Hoyer
Huffman
Israel
Jackson Lee
Jeffries
Johnson (GA)
Johnson, E. B.
Kaptur
Keating
Kelly (IL)
Kennedy
Kildee
Kilmer
Kind
Kirkpatrick
Kuster
Langevin
Larsen (WA)
Larson (CT)
Lawrence
Lee
Levin
Lewis
Lieu, Ted
Lipinski
Loebsack
Lofgren
Lowenthal
Lowey
Lujan Grisham (NM)
Luján, Ben Ray (NM)
Lynch
Maloney, Carolyn
Maloney, Sean
Matsui
McCollum
McDermott
McGovern
McNerney
Meeks
Meng
Moore
Moulton
Nadler
Napolitano
Neal
Nolan
Norcross
O'Rourke
Pallone
Pascrell
Payne
Pelosi
Perlmutter
Peters
Pingree
Pocan
Polis
Price (NC)
Quigley
Rangel
Rice (NY)
Richmond
Roybal-Allard
Ruiz
Ruppersberger
Rush
Ryan (OH)
Sánchez, Linda T.
Sanchez, Loretta
Sarbanes
Schakowsky
Schiff
Schrader
Scott (VA)
Scott, David
Serrano
Sewell (AL)
Sherman
Sinema
Sires
Slaughter
Speier
Swalwell (CA)
Takai
Takano
Thompson (CA)
Thompson (MS)
Titus
Tonko
Torres
Tsongas
Van Hollen
Vargas
Veasey
Vela
Velázquez
Visclosky
Walz
Waters, Maxine
Watson Coleman
Welch
Wilson (FL)
Yarmuth

NOES—239

Abraham
Aderholt
Allen
Amash
Amodei
Babin
Barletta
Barr
Barton
Benishek
Bilirakis
Bishop (MI)
Bishop (UT)
Black
Blackburn
Blum
Bost
Boustany
Brat
Bridenstine
Brooks (AL)
Brooks (IN)
Buchanan
Buck
Bucshon
Burgess
Byrne
Calvert
Carter (GA)
Carter (TX)
Chabot
Chaffetz
Clawson (FL)
Coffman
Cole
Collins (GA)
Collins (NY)
Comstock
Conaway
Cook
Costello (PA)
Cramer
Crawford
Crenshaw
Culberson
Davis, Rodney
Denham
Dent
DeSantis
DesJarlais
Diaz-Balart
Dold
Duffy
Duncan (SC)
Duncan (TN)
Ellmers (NC)
Emmer (MN)
Farenthold
Fincher
Fitzpatrick
Fleischmann
Fleming
Flores
Forbes
Fortenberry
Foxx
Franks (AZ)
Frelinghuysen
Garrett
Gibbs
Gibson
Gohmert
Goodlatte
Gosar
Gowdy
Granger
Graves (GA)
Graves (LA)
Griffith
Grothman
Guinta
Guthrie
Hanna
Hardy
Harper
Harris
Hartzler
Heck (NV)
Hensarling
Herrera Beutler
Hice, Jody B.
Hill
Holding
Hudson
Huelskamp
Huizenga (MI)
Hultgren
Hunter
Hurd (TX)
Hurt (VA)
Issa
Jenkins (KS)
Jenkins (WV)
Johnson (OH)
Johnson, Sam
Jolly
Jones
Jordan
Joyce
Katko
Kelly (PA)
King (IA)
King (NY)
Kinzinger (IL)
Kline
Knight
Labrador
Lamborn
Lance
Latta
LoBiondo
Long
Loudermilk
Love
Lucas
Luetkemeyer
Lummis
MacArthur
Marchant
Marino
Massie
McCarthy
McCaul
McClintock
McHenry
McKinley
McMorris Rodgers
McSally
Meadows
Meehan
Messer
Mica
Miller (FL)
Miller (MI)
Moolenaar
Mooney (WV)
Mullin
Mulvaney
Murphy (PA)
Neugebauer
Newhouse
Noem
Nugent
Nunes
Palazzo
Palmer
Paulsen
Pearce
Perry
Peterson
Pittenger
Pitts
Poe (TX)
Poliquin
Pompeo
Posey
Price, Tom
Ratcliffe
Reed
Reichert
Renacci
Ribble
Rice (SC)
Rigell
Roby
Roe (TN)
Rogers (AL)
Rogers (KY)
Rohrabacher
Rokita
Rooney (FL)
Ros-Lehtinen
Roskam
Ross
Rothfus
Rouzer
Royce
Russell
Ryan (WI)
Salmon
Sanford
Scalise
Schweikert
Scott, Austin
Sensenbrenner
Sessions
Shimkus
Shuster
Simpson
Smith (MO)
Smith (NE)
Smith (NJ)
Smith (TX)
Stefanik
Stewart
Stivers
Stutzman
Thompson (PA)
Thornberry
Tiberi
Tipton
Trott
Turner
Upton
Valadao
Wagner
Walberg
Walden
Walker
Walorski
Walters, Mimi
Weber (TX)
Webster (FL)
Wenstrup
Westerman
Westmoreland
Whitfield
Williams
Wilson (SC)
Wittman
Womack
Woodall
Yoder
Yoho
Young (AK)
Young (IA)
Young (IN)
Zeldin
Zinke

NOT VOTING—9

Brady (TX)
Curbelo (FL)
Graves (MO)
Hastings
LaMalfa
Murphy (FL)
Olson
Smith (WA)
Wasserman Schultz

□ 1635

So the motion to recommit was rejected.

The result of the vote was announced as above recorded.

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 ayes appeared to have it.

RECORDED VOTE

Mr. SCHIFF. Mr. Speaker, I demand a recorded vote.

A recorded vote was ordered.

The SPEAKER pro tempore. This is a 5-minute vote.

The vote was taken by electronic device, and there were—ayes 307, noes 116, not voting 8, as follows:

[Roll No. 170]

AYES—307

Abraham
Adams
Aderholt
Aguilar
Allen
Amodei
Ashford
Babin
Barletta
Barr
Beatty
Benishek
Bera
Beyer
Bilirakis
Bishop (GA)
Bishop (MI)
Bishop (UT)
Black
Blackburn
Blum
Bost
Boustany
Boyle, Brendan F.
Brooks (AL)
Brooks (IN)
Brown (FL)
Brownley (CA)
Buck
Bucshon
Burgess
Bustos
Butterfield
Byrne
Calvert
Cárdenas
Carney
Carson (IN)
Carter (GA)
Carter (TX)
Castor (FL)
Castro (TX)
Chabot
Chaffetz
Clarke (NY)
Clay
Cleaver
Clyburn
Coffman
Cole
Collins (GA)
Collins (NY)
Comstock
Conaway
Connolly
Cook
Cooper
Costa
Costello (PA)
Cramer
Crawford
Crenshaw
Crowley
Cuellar
Culberson
Davis (CA)
Davis, Rodney
Delaney
Denham
Dent
DeSantis
DeSaulnier
Diaz-Balart
Dingell
Dold
Duckworth
Duffy
Duncan (TN)
Ellmers (NC)
Emmer (MN)
Engel
Farenthold
Farr
Fincher
Fitzpatrick
Fleischmann
Flores
Forbes
Fortenberry
Foster
Foxx
Frankel (FL)
Franks (AZ)
Frelinghuysen
Fudge
Gallego
Garamendi
Gibbs
Goodlatte
Gowdy
Graham
Granger
Graves (GA)
Green, Gene
Guthrie
Gutiérrez
Hanna
Hardy
Harper
Hartzler
Heck (NV)
Heck (WA)
Hensarling
Herrera Beutler
Higgins
Hill
Himes
Hinojosa
Holding
Hoyer
Hudson
Huizenga (MI)
Hultgren
Hunter
Hurd (TX)
Hurt (VA)
Israel
Jackson Lee
Jeffries
Jenkins (KS)
Jenkins (WV)
Johnson (OH)
Johnson, Sam
Jolly
Joyce
Kaptur
Katko

Keating	Mullin	Sensenbrenner
Kelly (IL)	Mulvaney	Sessions
Kelly (PA)	Murphy (PA)	Sewell (AL)
Kennedy	Neal	Shimkus
Kilmer	Neugebauer	Shuster
Kind	Newhouse	Simpson
King (IA)	Noem	Sinema
King (NY)	Norcross	Sires
Kinzinger (IL)	Nugent	Smith (MO)
Kirkpatrick	Nunes	Smith (NE)
Kline	Palazzo	Smith (NJ)
Knight	Palmer	Smith (TX)
Kuster	Pascrell	Speier
LaMalfa	Paulsen	Stefanik
Lamborn	Payne	Stewart
Lance	Pearce	Stivers
Langevin	Pelosi	Swalwell (CA)
Larsen (WA)	Perlmutter	Takai
Latta	Peters	Thompson (CA)
Lawrence	Peterson	Thompson (MS)
Levin	Pittenger	Thompson (PA)
Lipinski	Pitts	Thornberry
LoBiondo	Poliquin	Tiberi
Loebsack	Pompeo	Tipton
Long	Price (NC)	Titus
Love	Price, Tom	Torres
Lowey	Quigley	Trott
Lucas	Ratcliffe	Turner
Luetkemeyer	Reed	Upton
Lujan Grisham (NM)	Reichert	Valadao
	Renacci	Vargas
Luján, Ben Ray (NM)	Rice (NY)	Veasey
	Rice (SC)	Visclosky
MacArthur	Richmond	Wagner
Maloney, Carolyn	Rigell	Walberg
	Roby	Walden
Maloney, Sean	Roe (TN)	Walker
Marchant	Rogers (AL)	Walorski
Marino	Rogers (KY)	Walters, Mimi
McCarthy	Rohrabacher	Weber (TX)
McCaul	Rokita	Webster (FL)
McHenry	Rooney (FL)	Wenstrup
McKinley	Ros-Lehtinen	Westerman
McMorris Rodgers	Roskam	Westmoreland
	Ross	Whitfield
McNerney	Rothfus	Williams
McSally	Rouzer	Wilson (FL)
Meadows	Royce	Wilson (SC)
Meehan	Ruiz	Wittman
Meeks	Ruppersberger	Womack
Meng	Russell	Woodall
Messer	Ryan (WI)	Yoder
Mica	Sanchez, Loretta	Yoho
Miller (FL)	Scalise	Young (AK)
Miller (MI)	Schiff	Young (IA)
Moolenaar	Schrader	Young (IN)
Moore	Scott, Austin	Zeldin
Moulton	Scott, David	Zinke

NOES—116

Amash	Gabbard	McDermott
Barton	Garrett	McGovern
Bass	Gibson	Mooney (WV)
Becerra	Gohmert	Nadler
Blumenauer	Gosar	Napolitano
Bonamici	Graves (LA)	Nolan
Brady (PA)	Grayson	O'Rourke
Brat	Green, Al	Pallone
Bridenstine	Griffith	Perry
Buchanan	Grijalva	Pingree
Capps	Grothman	Pocan
Capuano	Guinta	Poe (TX)
Cartwright	Hahn	Polis
Chu, Judy	Harris	Posey
Cicilline	Hice, Jody B.	Rangel
Clark (MA)	Honda	Ribble
Clawson (FL)	Huelskamp	Roybal-Allard
Cohen	Huffman	Rush
Conyers	Issa	Ryan (OH)
Courtney	Johnson (GA)	Salmon
Cummings	Johnson, E. B.	Sánchez, Linda T.
Davis, Danny	Jones	
DeFazio	Jordan	Sanford
DeGette	Kildee	Sarbanes
DeLauro	Labrador	Schakowsky
DelBene	Larson (CT)	Schweikert
DesJarlais	Lee	Scott (VA)
Deutch	Lewis	Serrano
Doggett	Lieu, Ted	Sherman
Doyle, Michael F.	Lofgren	Slaughter
	Loudermilk	Stutzman
Duncan (SC)	Lowenthal	Takano
Edwards	Lummis	Tonko
Ellison	Lynch	Tsongas
Eshoo	Massie	Van Hollen
Esty	Matsui	Vela
Fattah	McClintock	Velázquez
Fleming	McCollum	Walz
Waters, Maxine	Welch	
Watson Coleman	Yarmuth	

NOT VOTING—8

Brady (TX)	Hastings	Smith (WA)
Curbelo (FL)	Murphy (FL)	Wasserman Schultz
Graves (MO)	Olson	

□ 1642

So the bill was passed.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

HOUR OF MEETING ON TOMORROW

Mr. ROONEY of Florida. Mr. Speaker, I ask unanimous consent that when the House adjourns today, it adjourn to meet at 9 a.m. tomorrow.

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

There was no objection.

MOMENT OF SILENCE COMMEMORATING 100-YEAR ANNIVERSARY OF FIRST USE OF POISON GAS

(Mr. FOSTER asked and was given permission to address the House for 1 minute.)

Mr. FOSTER. Mr. Speaker, today represents the 100-year anniversary of the first use of poison gas on Earth. On April 22, 1915, chlorine gas was sent crawling in favorable winds over Flanders Fields from German positions into positions held by the French. This sowed terror and agony for the first time.

I would like for everyone present and everyone listening to pause for a moment to think of everyone who has died in the last 100 years from poison gas, including everyone who is dying today in Syria.

Mr. Speaker, many people in America were horrified at the ''60 Minutes'' presentation of the sarin attacks and the footage that that included. It is horrifying to think that chlorine is also being used in that war today.

There is a reason that we put chemical weapons in a separate category, never to be used by any nation in any war. Let us just pause and think for a moment and rededicate ourselves to ridding the entire world of chemical weapons forever.

□ 1645

TRIBUTE TO ED MEAD

(Mr. KELLY of Pennsylvania asked and was given permission to address the House for 1 minute.)

Mr. KELLY of Pennsylvania. Mr. Speaker, last month, our world bid farewell to Ed Mead, a former president, copublisher, editor, columnist, and all-around legend of the Erie Times-News in Erie, Pennsylvania, a paper founded by his grandfather in 1888.

Mr. Mead leaves behind an extraordinary legacy in the newspaper business and in the community of Erie, the city where he was born and spent so much of his life devoted to connecting with people.

Mr. Mead was often referred to as ''the voice of Erie,'' leading a long and distinguished career that included more than 14,000 features for his ''Odds and Ends'' column, one that appealed to so many people throughout our region.

Mr. Mead was so committed to serving his family's newspaper that, after graduating from Princeton University in 1949, he turned down a contract to play professional football in the National Football League's Detroit Lions club; instead, he decided to return to work in Erie for the next 63 years at the Erie Times.

Although Mr. Mead's passing will long be felt at the Erie Times Publishing Company and in the entire city of Erie and in the entire community, we know he now rests in heaven.

As is true of all legends, Ed Mead may be gone, but he will surely never be forgotten.

PINELLAS PARK POLICE CHIEF DORENE THOMAS

(Mr. JOLLY asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. JOLLY. Mr. Speaker, I rise today to recognize someone who has been described as a trailblazer, a pioneer, and a woman of firsts: Pinellas Park Police Chief Dorene Thomas who, on this Friday, will retire after four decades of public service.

Thomas became the first sworn female police officer at the Pinellas Park Police Department in 1980. In fact, when she started, the evidence room was located in the men's locker room, something she would eventually change.

In 2000, Thomas became the department's first female police chief, but she often said she would simply prefer to be known as a good police chief rather than a female police chief.

Five years ago, she was elected president of the Florida Police Chiefs Association, another first for women. She has also started intensive crisis intervention training, which teaches officers how to work with people with behavioral or mental health challenges.

Mr. Speaker, it is a privilege to recognize a person who has helped keep our citizens safe, to honor a person who has led with courage, kindness, grace, and understanding.

I urge my colleagues to join me in thanking Chief Thomas for her selfless years of service. Thank you for making Pinellas County a safer place, and thank you to all the men and women who, today, serve on the front lines of law enforcement.

Chief Thomas, enjoy your retirement. You have very well earned it.