This really has been a tremendous effort, and so important for our country. This particular issue, obviously, is certainly a bipartisan issue.

I say that, Mr. Chairman, because our Constitution makes the first and foremost responsibility of the Federal Government to provide for the common defense. That is actually in the preamble of our Constitution.

In our modern world, those who are seeking harm to our Nation, to our citizens, to our companies, can use many different means, including attacks over the Internet to attack our Nation.

Recent cyber attacks on U.S. companies like Sony, Target, and Home Depot not only harm these companies, Mr. Chairman, but they harm the American citizens who do business with them, putting their most personal private information at risk.

These threats, as are well known, are coming from nation-states like North Korea, Russia, Iran, China, as well as cyber criminals seeking to steal not only personal information but also intellectual property and sensitive government information.

In today's digital world, we have a duty to defend ourselves against cyber espionage, and the best way to combat these threats is to first recognize the threat and combine private and government resources and intelligence. Mr. Chairman, that is exactly what this bill does.

Mr. Chairman, I think this bill will help to facilitate greater cooperation and efforts to protect our Nation's digital infrastructure, including power grids and other utilities and other services that everyday Americans rely on each and every day.

By removing barriers, which will allow private companies to voluntarily share their cybersecurity threat information with the Department of Homeland Security and/or other companies, I think we will in a very large way improve earlier detection and mitigation of potential threats.

Additionally, this legislation that we are debating on the floor today ensures that personal identification information is removed prior to sharing information related to cyber threats and that very strong safeguards are in place to protect personal privacy and civil liberties.

Mr. Chairman, I point that out because that was something that was discussed a lot by practically every member of the Homeland Security Committee. We were all very, very united on that issue. And I think that is an important critical component, a point to make, and it is reflected in this legislation.

As Mr. RATCLIFFE mentioned just earlier, 85 percent of America's critical infrastructure is owned and operated by the private sector—think about that, 85 percent—which means that cyber threats pose as much of an economic threat to the United States as they do to our security, and we have a constitutional responsibility, as I pointed out in the beginning, to protect ourselves, to protect our Nation, to protect our American citizens from this ever-evolving threat.

So, Mr. Chairman, I would urge that all of my colleagues join me, join all of us on our committee, in voting in favor of this important legislation that will provide an additional line, and a very important line, of defense against cyber attacks.

The CHAIR. The Committee will rise informally.

The Speaker pro tempore (Mr. LOUDERMILK) assumed the chair.

MESSAGE FROM THE SENATE

A message from the Senate by Ms. Curtis, one of its clerks, announced that the Senate has passed a bill of the following title in which the concurrence of the House is requested:

S. 178. An act to provide justice for the victims of trafficking.

The SPEAKER pro tempore. The Committee will resume its sitting.

NATIONAL CYBERSECURITY PROTECTION ADVANCEMENT ACT OF 2015

The Committee resumed its sitting.

Mr. THOMPSON of Mississippi. Mr. Chairman, I yield 2 minutes to the gentleman from Virginia (Mr. CONNOLLY).

Mr. CONNOLLY. I thank my dear friend from Mississippi (Mr. THOMPSON), and I commend him and the distinguished chairman of the committee, Mr. MCCAUL, for their wonderful work on this bill.

Mr. Chairman, we cannot wait. America cannot wait for a cyber Pearl Harbor. This issue—cybersecurity—may be the most complex and difficult challenge we confront long term as a nation.

In the wired 21st century, the line between our physical world and cyberspace continues to blur with every aspect of our lives, from social interaction to commerce. Yet the remarkable gains that have accompanied an increasingly digital and connected society also have opened up new, unprecedented vulnerabilities that threaten to undermine this progress and cause great harm to our country's national security, critical infrastructure, and economy.

□ 0945

It is long overdue for Congress to modernize our cyber laws to address those vulnerabilities present in both public and private networks. The bills before us this week are a step in the right direction, and I am glad to support them, but they are a first step.

Information sharing alone does not inoculate or even defend us from cyber attacks. Indeed, in the critical three P's of enhancing cybersecurity—people, policies, and practices—the measures before us make improvements primarily to policy.

I commend the two committees for working in a bipartisan fashion to improve privacy and transparency protections. More is still needed to safeguard the civil liberties of our constituents.

Further, I hope that the broad liability protections provided by these bills will, in fact, be narrowed upon further consultation with the Senate. Cybersecurity must be a shared public-private responsibility, and that includes the expectation and requirement that our partners will, in fact, take reasonable actions.

Moving forward, I hope Congress will build on this effort to address the security of critical infrastructure, the vast majority of which, as has been already pointed out, is owned and operated by the private sector.

The CHAIR. The time of the gentleman has expired.

Mr. THOMPSON of Mississippi. I yield the gentleman an additional 30 seconds.

Mr. CONNOLLY. We also need to strengthen our Nation's cyber workforce, devise effective data breach notification policies, and bring about a wholesale cultural revolution so that society fully understands the critical importance of good cyber hygiene.

The bottom line is that our vulnerability in cyberspace demands that we take decisive action and take it now, but much like the tactics used in effective cybersecurity, we must recognize that enhancing our cyber defenses is an iterative process that requires continuous effort.

I congratulate the staffs and the leadership of the committee.

Mr. MCCAUL. Mr. Chairman, I yield 5 minutes to the gentleman from Georgia (Mr. LOUDERMILK), a member of the Committee on Homeland Security.

Mr. LOUDERMILK. Mr. Chairman, over the past 40 years, we have experienced advancements in information technology that literally have transformed business, education, government; it has even transformed our culture.

Information research that only a couple of decades ago would take days, months, maybe even years to accomplish is available, quite literally, at our fingertips and instantaneously.

Other aspects of our lives have also been shaped by this immediate access to information. Shopping, you can go shopping without ever going to a store. You can conduct financial transactions without ever going to a bank. You can even have access to entertainment without ever going to a theater.

These advancements in technology have not only transformed the way we access and store information, but it has also transformed the way we communicate.

No longer is instantaneous voice-to-voice communication only available through a phone call, but people around the world instantly connect with one another with a variety of methods, from email, instant text messaging, even video conferencing, and

this can be all down while you are on the move. You don't even have to be chained to a desk or in your business office.

Really, every aspect of our culture has been affected by the advancements in information technology, and, for the most part, our lives have been improved by these advancements.

As an IT professional, with 30-plus years' experience in both the military and private sector, I know firsthand the benefits of this instant access to endless amounts of information, but, on the other hand, I know all too well the vulnerabilities of these systems.

For the past 20 years, I have assisted businesses and governments to automate their operations and ensure they can access their networks anytime and from anywhere.

However, this global access to information requires a global interconnection of these systems. At almost any time during the day, Americans are connected to this global network through their phones, tablets, health monitors, and car navigation systems. Even home security systems are now connected to the Internet.

We have become dependent on this interconnection and so have the businesses and government entities that provide crucial services that we rely on, but as our dependence on technology has grown, so have our vulnerabilities.

Cyberspace is the new battleground, a battleground for a multitude of adversaries. Foreign nations, international terrorist organizations, and organized crime regularly target our citizens, businesses, and government.

Unlike traditional combat operations, cyber attackers don't require sophisticated weaponry to carry out their warfare. On the cyber battlefield, a single individual with a laptop computer can wreak havoc on business, the economy, even our critical infrastructure.

In the past several months, we have seen an increasing number of cyber attacks on national security systems and private company networks, breaching critical information. Earlier this year, Anthem BlueCross BlueShield's IT system was hacked by a highly sophisticated cyber attacker, obtaining personal employee and consumer data, including names, Social Security numbers, and mailing addresses.

An old adage among IT professionals states: There are two types of computer users, those who have been hacked and those who don't know that they have been hacked.

Today, this is truer than ever before. The incredible advancements made by the IT industry over the past three decades have been predominantly due to the competitive nature of the free market.

Without the overbearing constraints of government bureaucracy, oversight, and regulation, technology entrepreneurs have had the freedom to bring new innovations to the market with little cost and in record amount of time.

It is clear that our greatest advancements in technology have come from the private sector. That is why it is imperative that the government partner with the private sector to combat cyber attacks against our Nation.

The bill being debated in this House today, the National Cybersecurity Protection Advancement Act, puts in place a framework for voluntary partnership between government and the private sector to share information to protect against and combat against cyber attacks.

Through this voluntary sharing of critical information, businesses and government will voluntarily work together to respond to attacks and to prevent our enemies from corrupting networks, attacking our highly sensitive data systems, and compromising our personal privacy information.

While protecting individual privacy, this legislation also includes liability protections for the sharing of cyber threat information and thereby promotes information sharing that enhances the national cybersecurity posture.

We are no longer solely dealing with groups of hackers and terrorists, but individuals who target large networks, corrupt our database, and get hold of private material.

With today's evolving technology, we must make sure we are affirming individual privacy rights and safeguarding both government and private sector databases from cyberterrorism.

Protecting the civil liberties of the citizens of the United States is a top priority for me, and it should be for this Congress.

The CHAIR. The time of the gentleman has expired.

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

Mr. LOUDERMILK. That is why I do support H.R. 1731, because it provides that framework of cooperation between the government and the private industry, and it provides the protections and liability protections our industries need.

We must have this bill. I do stand in support of it, and I thank you for allowing me this time to speak.

Mr. THOMPSON of Mississippi. Mr. Chairman, I have no additional requests for time, so I reserve the balance of my time.

Mr. MCCAUL. Mr. Chairman, I yield such time as he may consume to the gentleman from Texas (Mr. HURD), a member of the Homeland Security Committee.

Mr. HURD of Texas. Mr. Chairman, I have spent almost 9 years, or a little bit over 9 years, as an undercover officer in the CIA. I chased al Qaeda, Taliban. Towards the end of my career, we started spending a lot more time focusing on cyber criminals, Russian organized crime, state sponsors of terror like Iran.

What this bill does is it helps in the protection of our digital infrastructure, both public and private, against this increasing threat.

I had the opportunity to help build a cybersecurity company, and seeing the threats to our infrastructure is great. This bill, which I rise in support of, is going to create that framework in order for the public and the private sector to work together against these threats.

When I was doing this for a living, you give me enough time, I am going to get in your network. We have to change our mindset and begin with the presumption of breach. How do we stop someone? How do we detect someone getting in our system? How do we corral them? And how do we kick them off? H.R. 1731 is a great start in doing this and making sure that we have the right protections.

We also are helping small- and medium-sized businesses with this bill, making sure that a lot of them have the resources that some larger businesses do and making sure that the Department of Homeland Security is providing as much information to them so that they can keep their company and their customers safe.

I would like to commend everyone on both sides of the aisle that is working to make this bill happen, and I look forward to seeing this get past this House and our colleagues in the Senate.

Mr. THOMPSON of Mississippi. Mr. Chairman, I continue to reserve the balance of my time.

Mr. MCCAUL. Mr. Chairman, I have no further requests for time. I am prepared to close if the gentleman from Mississippi is prepared to close.

I reserve the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Chairman, I yield myself such time as I may consume.

As someone involved in this issue for many years, I am not surprised by the overwhelming support that H.R. 1731 has garnered. Today, the House has the opportunity to join with the President and stakeholders from across our critical infrastructure sectors to make our Nation more secure.

By casting a vote in favor of H.R. 1731, you will be putting the Department of Homeland Security, the Federal civilian lead for cyber information sharing, on a path to fully partnering with the private sector to protect the U.S. networks.

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

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

Mr. Chairman, we are at a pivotal moment today and face a stark reality. The cyber threats to America have gone from bad to severe, and in many ways, we are flying blind.

The current level of cyber threat information sharing won't cut it. In the same way that we failed to stop terrorist attacks in the past, we are not connecting the dots well enough to prevent digital assaults against our Nation's networks.

The information we need to stop destructive breaches is held in silos, rather than being shared, preventing us from mounting an aggressive defense. In fact, the majority of cyber intrusions go unreported, leaving our networks vulnerable to the same attacks. When sharing does happen, it is often too little and too late.

If we don't pass this legislation to enhance cyber threat information sharing, we will be failing the American people and ceding more ground to our adversaries.

I hope, today, that we have the momentum to reverse the tide and to do what the American people expect of us, pass prosecurity, proprivacy legislation to better safeguard our public and private networks. Our inaction would be a permission slip for criminals, hacktivists, terrorists, and nation-states to continue to steal our data and to do our people harm.

I appreciate the collaboration from Members across the aisle and from other committees in developing this legislation. I would like to specifically commend, again, subcommittee Chairman RATCLIFFE for his work on this bill, as well as our minority counterparts, including Ranking Member THOMPSON and subcommittee Ranking Member RICHMOND for their joint work on this bill.

Mr. Chairman, I urge my colleagues to pass H.R. 1731.

I yield back the balance of my time.

Mr. VAN HOLLEN. Mr. Chair, I rise today to oppose H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015. I commend Chairman MCCAUL and Ranking Member THOMPSON for crafting a cybersecurity bill that improves upon legislation this body has previously voted on, but ultimately I cannot support it in its current form.

As was the case with yesterday's bill, the Protecting Cyber Networks Act (H.R. 1560), I continue to have concerns about the ambiguous liability provisions in this legislation. Specifically, H.R. 1731 would grant immunity to companies for simply putting forth a ''good faith'' effort when reporting security threats to the Department of Homeland Security. Like H.R. 1560, companies would receive liability protection even if they fail to act on threat information in a timely manner. I was disappointed that Republicans did not allow a vote on any of the seven amendments offered to improve the liability provisions in this bill.

I strongly believe that we must take steps to protect against these cyber threats while not sacrificing our privacy and civil liberties. It is my hope that many of these murky liability provisions can be resolved in the Senate, but I cannot support this bill as it stands today.

THE CHAIR. All time for general debate has expired.

In lieu of the amendment in the nature of a substitute recommended by the Committee on Homeland Security, printed in the bill, it shall be in order to consider as an original bill, for the purpose of amendment under the 5-minute rule, an amendment in the nature of a substitute consisting of the text of Rules Committee Print 114–12. That amendment in the nature of a substitute shall be considered as read.

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

H.R. 1731

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''National Cybersecurity Protection Advancement Act of 2015''.

SEC. 2. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) DEFINITIONS.—

(1) IN GENERAL.—Subsection (a) of the second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148; relating to the National Cybersecurity and Communications Integration Center) is amended—

(A) in paragraph (3), by striking ''and'' at the end;

(B) in paragraph (4), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following new paragraphs:

''(5) the term 'cyber threat indicator' means technical information that is necessary to describe or identify—

''(A) a method for probing, monitoring, maintaining, or establishing network awareness of an information system for the purpose of discerning technical vulnerabilities of such information system, if such method is known or reasonably suspected of being associated with a known or suspected cybersecurity risk, including communications that reasonably appear to be transmitted for the purpose of gathering technical information related to a cybersecurity risk;

''(B) a method for defeating a technical or security control of an information system;

''(C) a technical vulnerability, including anomalous technical behavior that may become a 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 inadvertently enable the defeat of a technical or operational control;

''(E) 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 that is known or reasonably suspected of being associated with a known or suspected cybersecurity risk;

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

''(G) any other attribute of a cybersecurity risk that cannot be used to identify specific persons reasonably believed to be unrelated to such cybersecurity risk, if disclosure of such attribute is not otherwise prohibited by law; or

''(H) any combination of subparagraphs (A) through (G);

''(6) the term 'cybersecurity purpose' means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity risk or incident;

''(7)(A) except as provided in subparagraph (B), the term 'defensive measure' means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity risk or incident, or any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control;

''(B) such term does not include a measure that destroys, renders unusable, or substantially harms an information system or data on an information system not belonging to—

''(i) the non-Federal entity, not including a State, local, or tribal government, operating such measure; or

''(ii) another Federal entity or non-Federal entity that is authorized to provide consent and has provided such consent to the non-Federal entity referred to in clause (i);

''(8) the term 'network awareness' means to scan, identify, acquire, monitor, log, or analyze information that is stored on, processed by, or transiting an information system;

''(9)(A) the term 'private entity' means a non-Federal entity that is an individual or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or non-profit entity, including an officer, employee, or agent thereof;

''(B) such term includes a component of a State, local, or tribal government performing electric utility services;

''(10) the term 'security control' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentially, integrity, or availability of an information system or information that is stored on, processed by, or transiting an information system; and

''(11) the term 'sharing' means providing, receiving, and disseminating.''.

(b) AMENDMENT.—Subparagraph (B) of subsection (d)(1) of such second section 226 of the Homeland Security Act of 2002 is amended—

(1) in clause (i), by striking ''and local'' and inserting '', local, and tribal'';

(2) in clause (ii)—

(A) by inserting '', including information sharing and analysis centers'' before the semicolon; and

(B) by striking ''and'' at the end;

(3) in clause (iii), by striking the period at the end and inserting ''; and''; and

(4) by adding at the end the following new clause:

''(iv) private entities.''.

SEC. 3. INFORMATION SHARING STRUCTURE AND PROCESSES.

The second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148; relating to the National Cybersecurity and Communications Integration Center) is amended—

(1) in subsection (c)—

(A) in paragraph (1)—

(i) by striking ''a Federal civilian interface'' and inserting ''the lead Federal civilian interface''; and

(ii) by striking ''cybersecurity risks,'' and inserting ''cyber threat indicators, defensive measures, cybersecurity risks,'';

(B) in paragraph (3), by striking ''cybersecurity risks'' and inserting ''cyber threat indicators, defensive measures, cybersecurity risks,'';

(C) in paragraph (5)(A), by striking ''cybersecurity risks'' and inserting ''cyber threat indicators, defensive measures, cybersecurity risks,'';

(D) in paragraph (6)—

(i) by striking ''cybersecurity risks'' and inserting ''cyber threat indicators, defensive measures, cybersecurity risks,''; and

(ii) by striking ''and'' at the end;

(E) in paragraph (7)—

(i) in subparagraph (A), by striking ''and'' at the end;

(ii) in subparagraph (B), by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following new subparagraph:

''(C) sharing cyber threat indicators and defensive measures;''; and

(F) by adding at the end the following new paragraphs

''(8) engaging with international partners, in consultation with other appropriate agencies, to—

''(A) collaborate on cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents; and

''(B) enhance the security and resilience of global cybersecurity;

''(9) sharing cyber threat indicators, defensive measures, and other information related to cybersecurity risks and incidents with Federal and non-Federal entities, including across sectors of critical infrastructure and with State and major urban area fusion centers, as appropriate;

''(10) promptly notifying the Secretary and the Committee on Homeland Security of the House of Representatives and the Committee on

Homeland Security and Governmental Affairs of the Senate of any significant violations of the policies and procedures specified in subsection (i)(6)(A);

''(11) promptly notifying non-Federal entities that have shared cyber threat indicators or defensive measures that are known or determined to be in error or in contravention of the requirements of this section; and

''(12) participating, as appropriate, in exercises run by the Department's National Exercise Program.'';

(2) in subsection (d)—

(A) in subparagraph (D), by striking ''and'' at the end;

(B) by redesignating subparagraph (E) as subparagraph (J); and

(C) by inserting after subparagraph (D) the following new subparagraphs:

''(E) an entity that collaborates with State and local governments on cybersecurity risks and incidents, and has entered into a voluntary information sharing relationship with the Center;

''(F) a United States Computer Emergency Readiness Team that coordinates information related to cybersecurity risks and incidents, proactively and collaboratively addresses cybersecurity risks and incidents to the United States, collaboratively responds to cybersecurity risks and incidents, provides technical assistance, upon request, to information system owners and operators, and shares cyber threat indicators, defensive measures, analysis, or information related to cybersecurity risks and incidents in a timely manner;

''(G) the Industrial Control System Cyber Emergency Response Team that—

''(i) coordinates with industrial control systems owners and operators;

''(ii) provides training, upon request, to Federal entities and non-Federal entities on industrial control systems cybersecurity;

''(iii) collaboratively addresses cybersecurity risks and incidents to industrial control systems;

''(iv) provides technical assistance, upon request, to Federal entities and non-Federal entities relating to industrial control systems cybersecurity; and

''(v) shares cyber threat indicators, defensive measures, or information related to cybersecurity risks and incidents of industrial control systems in a timely fashion;

''(H) a National Coordinating Center for Communications that coordinates the protection, response, and recovery of emergency communications;

''(I) an entity that coordinates with small and medium-sized businesses; and'';

(3) in subsection (e)—

(A) in paragraph (1)—

(i) in subparagraph (A), by inserting ''cyber threat indicators, defensive measures, and'' before ''information'';

(ii) in subparagraph (B), by inserting ''cyber threat indicators, defensive measures, and'' before ''information'';

(iii) in subparagraph (F), by striking ''cybersecurity risks'' and inserting ''cyber threat indicators, defensive measures, cybersecurity risks,'';

(iv) in subparagraph (F), by striking ''and'' at the end;

(v) in subparagraph (G), by striking ''cybersecurity risks'' and inserting ''cyber threat indicators, defensive measures, cybersecurity risks,''; and

(vi) by adding at the end the following:

''(H) the Center ensures that it shares information relating to cybersecurity risks and incidents with small and medium-sized businesses, as appropriate; and

''(I) the Center designates an agency contact for non-Federal entities;'';

(B) in paragraph (2)—

(i) by striking ''cybersecurity risks'' and inserting ''cyber threat indicators, defensive measures, cybersecurity risks,''; and

(ii) by inserting ''or disclosure'' before the semicolon at the end; and

(C) in paragraph (3), by inserting before the period at the end the following: '', including by working with the Chief Privacy Officer appointed under section 222 to ensure that the Center follows the policies and procedures specified in subsection (i)(6)(A)''; and

(4) by adding at the end the following new subsections:

''(g) RAPID AUTOMATED SHARING.—

''(1) IN GENERAL.—The Under Secretary for Cybersecurity and Infrastructure Protection, in coordination with industry and other stakeholders, shall develop capabilities making use of existing information technology industry standards and best practices, as appropriate, that support and rapidly advance the development, adoption, and implementation of automated mechanisms for the timely sharing of cyber threat indicators and defensive measures to and from the Center and with each Federal agency designated as the 'Sector Specific Agency' for each critical infrastructure sector in accordance with subsection (h).

''(2) BIANNUAL REPORT.—The Under Secretary for Cybersecurity and Infrastructure Protection shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a biannual report on the status and progress of the development of the capability described in paragraph (1). Such reports shall be required until such capability is fully implemented.

''(h) SECTOR SPECIFIC AGENCIES.—The Secretary, in collaboration with the relevant critical infrastructure sector and the heads of other appropriate Federal agencies, shall recognize the Federal agency designated as of March 25, 2015, as the 'Sector Specific Agency' for each critical infrastructure sector designated in the Department's National Infrastructure Protection Plan. If the designated Sector Specific Agency for a particular critical infrastructure sector is the Department, for purposes of this section, the Secretary is deemed to be the head of such Sector Specific Agency and shall carry out this section. The Secretary, in coordination with the heads of each such Sector Specific Agency, shall—

''(1) support the security and resilience actives of the relevant critical infrastructure sector in accordance with this section;

''(2) provide institutional knowledge, specialized expertise, and technical assistance upon request to the relevant critical infrastructure sector; and

''(3) support the timely sharing of cyber threat indicators and defensive measures with the relevant critical infrastructure sector with the Center in accordance with this section.

''(i) VOLUNTARY INFORMATION SHARING PROCEDURES.—

''(1) PROCEDURES.—

''(A) IN GENERAL.—The Center may enter into a voluntary information sharing relationship with any consenting non-Federal entity for the sharing of cyber threat indicators and defensive measures for cybersecurity purposes in accordance with this section. Nothing in this section may be construed to require any non-Federal entity to enter into any such information sharing relationship with the Center or any other entity. The Center may terminate a voluntary information sharing relationship under this subsection if the Center determines that the non-Federal entity with which the Center has entered into such a relationship has, after repeated notice, repeatedly violated the terms of this subsection.

''(B) NATIONAL SECURITY.—The Secretary may decline to enter into a voluntary information sharing relationship under this subsection if the Secretary determines that such is appropriate for national security.

''(2) VOLUNTARY INFORMATION SHARING RELATIONSHIPS.—A voluntary information sharing relationship under this subsection may be characterized as an agreement described in this paragraph.

''(A) STANDARD AGREEMENT.—For the use of a non-Federal entity, the Center shall make available a standard agreement, consistent with this section, on the Department's website.

''(B) NEGOTIATED AGREEMENT.—At the request of a non-Federal entity, and if determined appropriate by the Center, the Department shall negotiate a non-standard agreement, consistent with this section.

''(C) EXISTING AGREEMENTS.—An agreement between the Center and a non-Federal entity that is entered into before the date of the enactment of this section, or such an agreement that is in effect before such date, shall be deemed in compliance with the requirements of this subsection, notwithstanding any other provision or requirement of this subsection. An agreement under this subsection shall include the relevant privacy protections as in effect under the Cooperative Research and Development Agreement for Cybersecurity Information Sharing and Collaboration, as of December 31, 2014. Nothing in this subsection may be construed to require a non-Federal entity to enter into either a standard or negotiated agreement to be in compliance with this subsection.

''(3) INFORMATION SHARING AUTHORIZATION.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), and notwithstanding any other provision of law, a non-Federal entity may, for cybersecurity purposes, share cyber threat indicators or defensive measures obtained on its own information system, or on an information system of another Federal entity or non-Federal entity, upon written consent of such other Federal entity or non-Federal entity or an authorized representative of such other Federal entity or non-Federal entity in accordance with this section with—

''(i) another non-Federal entity; or

''(ii) the Center, as provided in this section.

''(B) LAWFUL RESTRICTION.—A non-Federal entity receiving a cyber threat indicator or defensive measure from another Federal entity or non-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 Federal entity or non-Federal entity.

''(C) REMOVAL OF INFORMATION UNRELATED TO CYBERSECURITY RISKS OR INCIDENTS.—Federal entities and non-Federal entities shall, prior to such sharing, take reasonable efforts to remove information that can be used to identify specific persons and is reasonably believed at the time of sharing to be unrelated to a cybersecurity risks or incident and to safeguard information that can be used to identify specific persons from unintended disclosure or unauthorized access or acquisition.

''(D) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to—

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

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

''(iii) require a new information sharing relationship between any non-Federal entity and a Federal entity;

''(iv) limit otherwise lawful activity; or

''(v) in any manner impact or modify procedures in existence as of the date of the enactment of this section for reporting known or suspected criminal activity to appropriate law enforcement authorities or for participating voluntarily or under legal requirement in an investigation.

''(E) COORDINATED VULNERABILITY DISCLOSURE.—The Under Secretary for Cybersecurity and Infrastructure Protection, in coordination with industry and other stakeholders, shall develop, publish, and adhere to policies and procedures for coordinating vulnerability disclosures, to the extent practicable, consistent with international standards in the information technology industry.

''(4) NETWORK AWARENESS AUTHORIZATION.—

''(A) IN GENERAL.—Notwithstanding any other provision of law, a non-Federal entity, not including a State, local, or tribal government, may, for cybersecurity purposes, conduct network awareness of—

''(i) an information system of such non-Federal entity to protect the rights or property of such non-Federal entity;

''(ii) an information system of another non-Federal entity, upon written consent of such other non-Federal entity for conducting such network awareness to protect the rights or property of such other non-Federal entity;

''(iii) an information system of a Federal entity, upon written consent of an authorized representative of such Federal entity for conducting such network awareness to protect the rights or property of such Federal entity; or

''(iv) information that is stored on, processed by, or transiting an information system described in this subparagraph.

''(B) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to—

''(i) authorize conducting network awareness of an information system, or the use of any information obtained through such conducting of network awareness, other than as provided in this section; or

''(ii) limit otherwise lawful activity.

''(5) DEFENSIVE MEASURE AUTHORIZATION.—

''(A) IN GENERAL.—Except as provided in subparagraph (B) and notwithstanding any other provision of law, a non-Federal entity, not including a State, local, or tribal government, may, for cybersecurity purposes, operate a defensive measure that is applied to—

''(i) an information system of such non-Federal entity to protect the rights or property of such non-Federal entity;

''(ii) an information system of another non-Federal entity upon written consent of such other non-Federal entity for operation of such defensive measure to protect the rights or property of such other non-Federal entity;

''(iii) an information system of a Federal entity upon written consent of an authorized representative of such Federal entity for operation of such defensive measure to protect the rights or property of such Federal entity; or

''(iv) information that is stored on, processed by, or transiting an information system described in this subparagraph.

''(B) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to—

''(i) authorize the use of a defensive measure other than as provided in this section; or

''(ii) limit otherwise lawful activity.

''(6) PRIVACY AND CIVIL LIBERTIES PROTECTIONS.—

''(A) POLICIES AND PROCEDURES.—

''(i) IN GENERAL.—The Under Secretary for Cybersecurity and Infrastructure Protection shall, in coordination with the Chief Privacy Officer and the Chief Civil Rights and Civil Liberties Officer of the Department, establish and annually review policies and procedures governing the receipt, retention, use, and disclosure of cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents shared with the Center in accordance with this section. Such policies and procedures shall apply only to the Department, consistent with the need to protect information systems from cybersecurity risks and incidents and mitigate cybersecurity risks and incidents in a timely manner, and shall—

''(I) be consistent with the Department's Fair Information Practice Principles developed pursuant to section 552a of title 5, United States Code (commonly referred to as the 'Privacy Act of 1974' or the 'Privacy Act'), and subject to the Secretary's authority under subsection (a)(2) of section 222 of this Act;

''(II) reasonably limit, to the greatest extent practicable, the receipt, retention, use, and disclosure of cyber threat indicators and defensive measures associated with specific persons that is not necessary, for cybersecurity purposes, to protect a network or information system from cybersecurity risks or mitigate cybersecurity risks and incidents in a timely manner;

''(III) minimize any impact on privacy and civil liberties;

''(IV) provide data integrity through the prompt removal and destruction of obsolete or erroneous names and personal information that is unrelated to the cybersecurity risk or incident information shared and retained by the Center in accordance with this section;

''(V) include requirements to safeguard cyber threat indicators and defensive measures retained by the Center, including information that is proprietary or business-sensitive that may be used to identify specific persons from unauthorized access or acquisition;

''(VI) protect the confidentiality of cyber threat indicators and defensive measures associated with specific persons to the greatest extent practicable; and

''(VII) ensure all relevant constitutional, legal, and privacy protections are observed.

''(ii) SUBMISSION TO CONGRESS.—Not later than 180 days after the date of the enactment of this section and annually thereafter, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department, in consultation with the Privacy and Civil Liberties Oversight Board (established pursuant to section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee)), shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate the policies and procedures governing the sharing of cyber threat indicators, defensive measures, and information related to cybsersecurity risks and incidents described in clause (i) of subparagraph (A).

''(iii) PUBLIC NOTICE AND ACCESS.—The Under Secretary for Cybersecurity and Infrastructure Protection, in consultation with the Chief Privacy Officer and the Chief Civil Rights and Civil Liberties Officer of the Department, and the Privacy and Civil Liberties Oversight Board (established pursuant to section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee)), shall ensure there is public notice of, and access to, the policies and procedures governing the sharing of cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents.

''(iv) CONSULTATION.—The Under Secretary for Cybersecurity and Infrastructure Protection when establishing policies and procedures to support privacy and civil liberties may consult with the National Institute of Standards and Technology.

''(B) IMPLEMENTATION.—The Chief Privacy Officer of the Department, on an ongoing basis, shall—

''(i) monitor the implementation of the policies and procedures governing the sharing of cyber threat indicators and defensive measures established pursuant to clause (i) of subparagraph (A);

''(ii) regularly review and update privacy impact assessments, as appropriate, to ensure all relevant constitutional, legal, and privacy protections are being followed;

''(iii) work with the Under Secretary for Cybersecurity and Infrastructure Protection to carry out paragraphs (10) and (11) of subsection (c);

''(iv) annually submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that contains a review of the effectiveness of such policies and procedures to protect privacy and civil liberties; and

''(v) ensure there are appropriate sanctions in place for officers, employees, or agents of the Department who intentionally or willfully conduct activities under this section in an unauthorized manner.

''(C) INSPECTOR GENERAL REPORT.—The Inspector General of the Department, in consultation with the Privacy and Civil Liberties Oversight Board and the Inspector General of each Federal agency that receives cyber threat indicators or defensive measures shared with the Center under this section, shall, not later than two years after the date of the enactment of this subsection and periodically thereafter submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report containing a review of the use of cybersecurity risk information shared with the Center, including the following:

''(i) A report on the receipt, use, and dissemination of cyber threat indicators and defensive measures that have been shared with Federal entities under this section.

''(ii) Information on the use by the Center of such information for a purpose other than a cybersecurity purpose.

''(iii) A review of the type of information shared with the Center under this section.

''(iv) A review of the actions taken by the Center based on such information.

''(v) The appropriate metrics that exist to determine the impact, if any, on privacy and civil liberties as a result of the sharing of such information with the Center.

''(vi) A list of other Federal agencies receiving such information.

''(vii) A review of the sharing of such information within the Federal Government to identify inappropriate stove piping of such information.

''(viii) Any recommendations of the Inspector General of the Department for improvements or modifications to information sharing under this section.

''(D) PRIVACY AND CIVIL LIBERTIES OFFICERS REPORT.—The Chief Privacy Officer and the Chief Civil Rights and Civil Liberties Officer of the Department, in consultation with the Privacy and Civil Liberties Oversight Board, the Inspector General of the Department, and the senior privacy and civil liberties officer of each Federal agency that receives cyber threat indicators and defensive measures shared with the Center under this section, shall biennially submit to the appropriate congressional committees a report assessing the privacy and civil liberties impact of the activities under this paragraph. Each such report shall include any recommendations the Chief Privacy Officer and the Chief Civil Rights and Civil Liberties Officer of the Department consider appropriate to minimize or mitigate the privacy and civil liberties impact of the sharing of cyber threat indicators and defensive measures under this section.

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

''(7) USES AND PROTECTION OF INFORMATION.—

''(A) NON-FEDERAL ENTITIES.—A non-Federal entity, not including a State, local, or tribal government, that shares cyber threat indicators or defensive measures through the Center or otherwise under this section—

''(i) may use, retain, or further disclose such cyber threat indicators or defensive measures solely for cybersecurity purposes;

''(ii) shall, prior to such sharing, take reasonable efforts to remove information that can be used to identify specific persons and is reasonably believed at the time of sharing to be unrelated to a cybersecurity risk or incident, and to safeguard information that can be used to identify specific persons from unintended disclosure or unauthorized access or acquisition;

''(iii) shall comply with appropriate restrictions that a Federal entity or non-Federal entity places on the subsequent disclosure or retention of cyber threat indicators and defensive measures that it discloses to other Federal entities or non-Federal entities;

''(iv) shall be deemed to have voluntarily shared such cyber threat indicators or defensive measures;

''(v) shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures; and

''(vi) may not use such information to gain an unfair competitive advantage to the detriment of any non-Federal entity.

''(B) FEDERAL ENTITIES.—

''(i) USES OF INFORMATION.—A Federal entity that receives cyber threat indicators or defensive measures shared through the Center or otherwise under this section from another Federal entity or a non-Federal entity—

''(I) may use, retain, or further disclose such cyber threat indicators or defensive measures solely for cybersecurity purposes;

''(II) shall, prior to such sharing, take reasonable efforts to remove information that can be used to identify specific persons and is reasonably believed at the time of sharing to be unrelated to a cybersecurity risk or incident, and to safeguard information that can be used to identify specific persons from unintended disclosure or unauthorized access or acquisition;

''(III) shall be deemed to have voluntarily shared such cyber threat indicators or defensive measures;

''(IV) shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures; and

''(V) may not use such cyber threat indicators or defensive measures to engage in surveillance or other collection activities for the purpose of tracking an individual's personally identifiable information.

''(ii) PROTECTIONS FOR INFORMATION.—The cyber threat indicators and defensive measures referred to in clause (i)—

''(I) are exempt from disclosure under section 552 of title 5, United States Code, and withheld, without discretion, from the public under subsection (b)(3)(B) of such section;

''(II) may not be used by the Federal Government for regulatory purposes;

''(III) may not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection;

''(IV) shall be considered the commercial, financial, and proprietary information of the non-Federal entity referred to in clause (i) when so designated by such non-Federal entity; and

''(V) may not be subject to a rule of any Federal entity or any judicial doctrine regarding ex parte communications with a decisionmaking official.

''(C) STATE, LOCAL, OR TRIBAL GOVERNMENT.—

''(i) USES OF INFORMATION.—A State, local, or tribal government that receives cyber threat indicators or defensive measures from the Center from a Federal entity or a non-Federal entity—

''(I) may use, retain, or further disclose such cyber threat indicators or defensive measures solely for cybersecurity purposes;

''(II) shall, prior to such sharing, take reasonable efforts to remove information that can be used to identify specific persons and is reasonably believed at the time of sharing to be unrelated to a cybersecurity risk or incident, and to safeguard information that can be used to identify specific persons from unintended disclosure or unauthorized access or acquisition;

''(III) shall consider such information the commercial, financial, and proprietary information of such Federal entity or non-Federal entity if so designated by such Federal entity or non-Federal entity;

''(IV) shall be deemed to have voluntarily shared such cyber threat indicators or defensive measures; and

''(V) shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures.

''(ii) PROTECTIONS FOR INFORMATION.—The cyber threat indicators and defensive measures referred to in clause (i)—

''(I) shall be exempt from disclosure under any State, local, or tribal law or regulation that requires public disclosure of information or records by a public or quasi-public entity; and

''(II) may not be used by any State, local, or tribal government to regulate a lawful activity of a non-Federal entity.

''(8) LIABILITY EXEMPTIONS.—

''(A) NETWORK AWARENESS.—No cause of action shall lie or be maintained in any court, and such action shall be promptly dismissed, against any non-Federal entity that, for cybersecurity purposes, conducts network awareness under paragraph (4), if such network awareness is conducted in accordance with such paragraph and this section.

''(B) INFORMATION SHARING.—No cause of action shall lie or be maintained in any court, and such action shall be promptly dismissed, against any non-Federal entity that, for cybersecurity purposes, shares cyber threat indicators or defensive measures under paragraph (3), or fails to act based on such sharing, if such sharing is conducted in accordance with such paragraph and this section.

''(C) WILLFUL MISCONDUCT.—

''(i) RULE OF CONSTRUCTION.—Nothing in this section may be construed to—

''(I) require dismissal of a cause of action against a non-Federal entity that has engaged in willful misconduct in the course of conducting activities authorized by this section; or

''(II) undermine or limit the availability of otherwise applicable common law or statutory defenses.

''(ii) PROOF OF WILLFUL MISCONDUCT.—In any action claiming that subparagraph (A) or (B) does not apply due to willful misconduct described in clause (i), 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.

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

''(I) intentionally to achieve a wrongful purpose;

''(II) knowingly without legal or factual justification; and

''(III) 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.

''(D) EXCLUSION.—The term 'non-Federal entity' as used in this paragraph shall not include a State, local, or tribal government.

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

''(A) IN GENERAL.—If a department or agency of the Federal Government intentionally or willfully violates the restrictions specified in paragraph (3), (6), or (7)(B) on the use and protection of voluntarily shared cyber threat indicators or defensive measures, or any other provision of this section, the Federal Government shall be liable to a person injured by such violation in an amount equal to the sum of—

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

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

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

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

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

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

''(iv) 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 any restriction specified in paragraph (3), (6), or 7(B), or any other provision of this section, that is the basis for such 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 of any restriction specified in paragraph (3), (6), or 7(B) or any other provision of this section.

''(10) ANTI-TRUST EXEMPTION.—

''(A) IN GENERAL.—Except as provided in subparagraph (C), it shall not be considered a violation of any provision of antitrust laws for two or more non-Federal entities to share a cyber threat indicator or defensive measure, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity risk or incident, for cybersecurity purposes under this Act.

''(B) APPLICABILITY.—Subparagraph (A) shall apply only to information that is shared or assistance that is provided in order to assist with—

''(i) facilitating the prevention, investigation, or mitigation of a cybersecurity risk or incident to an information system or information that is stored on, processed by, or transiting an information system; or

''(ii) communicating or disclosing a cyber threat indicator or defensive measure to help prevent, investigate, or mitigate the effect of a cybersecurity risk or incident to an information system or information that is stored on, processed by, or transiting an information system.

''(C) PROHIBITED CONDUCT.—Nothing in this section may be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

''(11) CONSTRUCTION AND PREEMPTION.—

''(A) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this section may be construed to limit or prohibit otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity or participating voluntarily or under legal requirement in an investigation, by a non-Federal to any other non-Federal entity or Federal entity under this section.

''(B) WHISTLE BLOWER PROTECTIONS.—Nothing in this section may 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), section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) (governing disclosure by employees of elements of the intelligence community), or any similar provision of Federal or State law.

''(C) RELATIONSHIP TO OTHER LAWS.—Nothing in this section may be construed to affect any requirement under any other provision of law for a non-Federal entity to provide information to a Federal entity.

''(D) PRESERVATION OF CONTRACTUAL OBLIGATIONS AND RIGHTS.—Nothing in this section may be construed to—

''(i) 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

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

''(E) ANTI-TASKING RESTRICTION.—Nothing in this section may be construed to permit a Federal entity to—

''(i) require a non-Federal entity to provide information to a Federal entity;

''(ii) condition the sharing of cyber threat indicators or defensive measures with a non-Federal entity on such non-Federal entity's provision of cyber threat indicators or defensive measures to a Federal entity; or

''(iii) condition the award of any Federal grant, contract, or purchase on the sharing of cyber threat indicators or defensive measures with a Federal entity.

''(F) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this section may be construed to subject any non-Federal entity to liability for choosing to not engage in the voluntary activities authorized under this section.

''(G) USE AND RETENTION OF INFORMATION.—Nothing in this section may 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 section for any use other than permitted in this section.

''(H) VOLUNTARY SHARING.—Nothing in this section may be construed to restrict or condition a non-Federal entity from sharing, for cybersecurity purposes, cyber threat indicators, defensive measures, or information related to cybersecurity risks or incidents with any other non-Federal entity, and nothing in this section may be construed as requiring any non-Federal entity to share cyber threat indicators, defensive measures, or information related to cybersecurity risks or incidents with the Center.

''(I) FEDERAL PREEMPTION.—This section supersedes 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 section.

''(j) DIRECT REPORTING.—The Secretary shall develop policies and procedures for direct reporting to the Secretary by the Director of the Center regarding significant cybersecurity risks and incidents.

''(k) ADDITIONAL RESPONSIBILITIES.—The Secretary shall build upon existing mechanisms to promote a national awareness effort to educate the general public on the importance of securing information systems.

''(l) REPORTS ON INTERNATIONAL COOPERATION.—Not later than 180 days after the date of the enactment of this subsection and periodically thereafter, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the range of efforts underway to bolster cybersecurity collaboration with relevant international partners in accordance with subsection (c)(8).

''(m) OUTREACH.—Not later than 60 days after the date of the enactment of this subsection, the Secretary, acting through the Under Secretary for Cybersecurity and Infrastructure Protection, shall—

''(1) disseminate to the public information about how to voluntarily share cyber threat indicators and defensive measures with the Center; and

''(2) enhance outreach to critical infrastructure owners and operators for purposes of such sharing.''.

SEC. 4. INFORMATION SHARING AND ANALYSIS ORGANIZATIONS.

Section 212 of the Homeland Security Act of 2002 (6 U.S.C. 131) is amended—

(1) in paragraph (5)—

(A) in subparagraph (A)—

(i) by inserting ''information related to cybersecurity risks and incidents and'' after ''critical infrastructure information''; and

(ii) by striking ''related to critical infrastructure'' and inserting ''related to cybersecurity risks, incidents, critical infrastructure, and'';

(B) in subparagraph (B)—

(i) by striking ''disclosing critical infrastructure information'' and inserting ''disclosing cybersecurity risks, incidents, and critical infrastructure information''; and

(ii) by striking ''related to critical infrastructure or'' and inserting ''related to cybersecurity risks, incidents, critical infrastructure, or'' and

(C) in subparagraph (C), by striking ''disseminating critical infrastructure information'' and inserting ''disseminating cybersecurity risks, incidents, and critical infrastructure information''; and

(2) by adding at the end the following new paragraph:

''(8) CYBERSECURITY RISK; INCIDENT.—The terms 'cybersecurity risk' and 'incident' have the meanings given such terms in the second section 226 (relating to the National Cybersecurity and Communications Integration Center).''.

SEC. 5. STREAMLINING OF DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AND INFRASTRUCTURE PROTECTION ORGANIZATION.

(a) CYBERSECURITY AND INFRASTRUCTURE PROTECTION.—The National Protection and Programs Directorate of the Department of Homeland Security shall, after the date of the enactment of this Act, be known and designated as the ''Cybersecurity and Infrastructure Protection''. Any reference to the National Protection and Programs Directorate of the Department in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Cybersecurity and Infrastructure Protection of the Department.

(b) SENIOR LEADERSHIP OF CYBERSECURITY AND INFRASTRUCTURE PROTECTION.—

(1) IN GENERAL.—Subsection (a) of section 103 of the Homeland Security Act of 2002 (6 U.S.C. 113) is amended—

(A) in paragraph (1)—

(i) by amending subparagraph (H) to read as follows:

''(H) An Under Secretary for Cybersecurity and Infrastructure Protection.''; and

(ii) by adding at the end the following new subparagraphs:

''(K) A Deputy Under Secretary for Cybersecurity.

''(L) A Deputy Under Secretary for Infrastructure Protection.''; and

(B) by adding at the end the following new paragraph:

''(3) DEPUTY UNDER SECRETARIES.—The Deputy Under Secretaries referred to in subparagraphs (K) and (L) of paragraph (1) shall be appointed by the President without the advice and consent of the Senate.''.

(2) CONTINUATION IN OFFICE.—The individuals who hold the positions referred in subparagraphs (H), (K), and (L) of paragraph (1) of section 103(a) the Homeland Security Act of 2002 (as amended and added by paragraph (1) of this subsection) as of the date of the enactment of this Act may continue to hold such positions.

(c) REPORT.—Not later than 90 days after the date of the enactment of this Act, the Under Secretary for Cybersecurity and Infrastructure Protection of the Department of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the feasibility of becoming an operational component, including an analysis of alternatives, and if a determination is rendered that becoming an operational component is the best option for achieving the mission of Cybersecurity and Infrastructure Protection, a legislative proposal and implementation plan for becoming such an operational component. Such report shall also include plans to more effectively carry out the cybersecurity mission of Cybersecurity and Infrastructure Protection, including expediting information sharing agreements.

SEC. 6. CYBER INCIDENT RESPONSE PLANS.

(a) IN GENERAL.—Section 227 of the Homeland Security Act of 2002 (6 U.S.C. 149) is amended—

(1) in the heading, by striking ''**PLAN**'' and inserting ''**PLANS**'';

(2) by striking ''The Under Secretary appointed under section 103(a)(1)(H) shall'' and inserting the following:

''(a) IN GENERAL.—The Under Secretary for Cybersecurity and Infrastructure Protection shall''; and

(3) by adding at the end the following new subsection:

''(b) UPDATES TO THE CYBER INCIDENT ANNEX TO THE NATIONAL RESPONSE FRAMEWORK.—The Secretary, in coordination with the heads of other appropriate Federal departments and agencies, and in accordance with the National Cybersecurity Incident Response Plan required under subsection (a), shall regularly update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.''.

(b) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by amending the item relating to section 227 to read as follows:

''Sec. 227. Cyber incident response plans.''.

SEC. 7. SECURITY AND RESILIENCY OF PUBLIC SAFETY COMMUNICATIONS; CYBERSECURITY AWARENESS CAMPAIGN.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended by adding at the end the following new sections:

''SEC. 230. SECURITY AND RESILIENCY OF PUBLIC SAFETY COMMUNICATIONS.

''The National Cybersecurity and Communications Integration Center, in coordination with the Office of Emergency Communications of the Department, shall assess and evaluate consequence, vulnerability, and threat information regarding cyber incidents to public safety communications to help facilitate continuous improvements to the security and resiliency of such communications.

''SEC. 231. CYBERSECURITY AWARENESS CAMPAIGN.

''(a) IN GENERAL.—The Under Secretary for Cybersecurity and Infrastructure Protection shall develop and implement an ongoing and comprehensive cybersecurity awareness campaign regarding cybersecurity risks and voluntary best practices for mitigating and responding to such risks. Such campaign shall, at a minimum, publish and disseminate, on an ongoing basis, the following:

''(1) Public service announcements targeted at improving awareness among State, local, and tribal governments, the private sector, academia, and stakeholders in specific audiences, including the elderly, students, small businesses, members of the Armed Forces, and veterans.

''(2) Vendor and technology-neutral voluntary best practices information.

''(b) CONSULTATION.—The Under Secretary for Cybersecurity and Infrastructure Protection shall consult with a wide range of stakeholders in government, industry, academia, and the non-profit community in carrying out this section.''.

(b) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 226 (relating to cybersecurity recruitment and retention) the following new items:

''Sec. 230. Security and resiliency of public safety communications.

''Sec. 231. Cybersecurity awareness campaign.''.

SEC. 8. CRITICAL INFRASTRUCTURE PROTECTION RESEARCH AND DEVELOPMENT.

(a) STRATEGIC PLAN; PUBLIC-PRIVATE CONSORTIUMS.—Title III of the Homeland Security Act of 2002 (6 U.S.C. 181 et seq.) is amended by adding at the end the following new section:

''SEC. 318. RESEARCH AND DEVELOPMENT STRATEGY FOR CRITICAL INFRASTRUCTURE PROTECTION.

''(a) IN GENERAL.—Not later than 180 days after the date of enactment of this section, the Secretary, acting through the Under Secretary for Science and Technology, shall submit to

Congress a strategic plan to guide the overall direction of Federal physical security and cybersecurity technology research and development efforts for protecting critical infrastructure, including against all threats. Such plan shall be updated and submitted to Congress every two years.

''(b) CONTENTS OF PLAN.—The strategic plan, including biennial updates, required under subsection (a) shall include the following:

''(1) An identification of critical infrastructure security risks and any associated security technology gaps, that are developed following—

''(A) consultation with stakeholders, including critical infrastructure Sector Coordinating Councils; and

''(B) performance by the Department of a risk and gap analysis that considers information received in such consultations.

''(2) A set of critical infrastructure security technology needs that—

''(A) is prioritized based on the risks and gaps identified under paragraph (1);

''(B) emphasizes research and development of technologies that need to be accelerated due to rapidly evolving threats or rapidly advancing infrastructure technology; and

''(C) includes research, development, and acquisition roadmaps with clearly defined objectives, goals, and measures.

''(3) An identification of laboratories, facilities, modeling, and simulation capabilities that will be required to support the research, development, demonstration, testing, evaluation, and acquisition of the security technologies described in paragraph (2).

''(4) An identification of current and planned programmatic initiatives for fostering the rapid advancement and deployment of security technologies for critical infrastructure protection, including a consideration of opportunities for public-private partnerships, intragovernment collaboration, university centers of excellence, and national laboratory technology transfer.

''(5) A description of progress made with respect to each critical infrastructure security risk, associated security technology gap, and critical infrastructure technology need identified in the preceding strategic plan required under subsection (a).

''(c) COORDINATION.—In carrying out this section, the Under Secretary for Science and Technology shall coordinate with the Under Secretary for the National Protection and Programs Directorate.

''(d) CONSULTATION.—In carrying out this section, the Under Secretary for Science and Technology shall consult with—

''(1) critical infrastructure Sector Coordinating Councils;

''(2) to the extent practicable, subject matter experts on critical infrastructure protection from universities, colleges, national laboratories, and private industry;

''(3) the heads of other relevant Federal departments and agencies that conduct research and development relating to critical infrastructure protection; and

''(4) State, local, and tribal governments, as appropriate.''.

(b) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 317 the following new item:

''Sec. 318. Research and development strategy for critical infrastructure protection.''.

SEC. 9. REPORT ON REDUCING CYBERSECURITY RISKS IN DHS DATA CENTERS.

Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the feasibility of the Department of Homeland Security creating an environment for the reduction in cybersecurity risks in Department data centers, including by increasing compartmentalization between systems, and providing a mix of security controls between such compartments.

SEC. 10. ASSESSMENT.

Not later than two years after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that contains an assessment of the implementation by the Secretary of Homeland Security of this Act and the amendments made by this Act and, to the extent practicable, findings regarding increases in the sharing of cyber threat indicators, defensive measures, and information relating to cybersecurity risks and incidents at the National Cybersecurity and Communications Integration Center and throughout the United States.

SEC. 11. CONSULTATION.

The Under Secretary for Cybersecurity and Infrastructure Protection shall produce a report on the feasibility of creating a risk-informed prioritization plan should multiple critical infrastructures experience cyber incidents simultaneously.

SEC. 12. TECHNICAL ASSISTANCE.

The Inspector General of the Department of Homeland Security shall review the operations of the United States Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to assess the capacity to provide technical assistance to non-Federal entities and to adequately respond to potential increases in requests for technical assistance.

SEC. 13. PROHIBITION ON NEW REGULATORY AUTHORITY.

Nothing in this Act or the amendments made by this Act may be construed to grant the Secretary of Homeland Security any authority to promulgate regulations or set standards relating to the cybersecurity of non-Federal entities, not including State, local, and tribal governments, that was not in effect on the day before the date of the enactment of this Act.

SEC. 14. SUNSET.

Any requirements for reports required by this Act or the amendments made by this Act shall terminate on the date that is seven years after the date of the enactment of this Act.

SEC. 15. PROHIBITION ON NEW FUNDING.

No funds are authorized to be appropriated to carry out this Act and the amendments made by this Act. This Act and such amendments shall be carried out using amounts appropriated or otherwise made available for such purposes.

The CHAIR. No amendment to that amendment in the nature of a substitute shall be in order except those printed in part B 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 as read, shall be debatable for the time specified in the report, equally divided and controlled by the proponent and an opponent, shall not be subject to amendment, and shall not be subject to a demand for division of the question.

□ 1000

AMENDMENT NO. 1 OFFERED BY MR. MCCAUL

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

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

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

In section 2, strike the following:

(a) DEFINITIONS.—

(1) IN GENERAL.—Subsection (a) of the second section 226

In section 2, insert before subsection (b), the following:

(a) IN GENERAL.—Subsection (a) of the second section 226

In section 2(a), redesignate proposed subparagraphs (A) through (C) as proposed paragraphs (1) through (3), respectively, and move such provisions two ems to the left.

Page 3, line 23, insert '', or the purpose of identifying the source of a cybersecurity risk or incident'' before the semicolon at the end.

Page 5, beginning line 6, strike ''electric utility services'' and insert ''utility services or an entity performing utility services''.

Page 5, line 15, insert ''(including all conjugations thereof)'' before ''means''.

Page 5, line 16, insert ''(including all conjugations of each of such terms)'' before the first period.

Page 6, beginning line 2, strike ''striking the period at the end and inserting '; and'' and insert ''inserting 'and' after the semicolon at the end''.

Page 6, line 6, strike the first period and insert a semicolon.

Page 7, line 20, insert a colon after ''paragraphs''.

Page 8, line 23, strike ''(d)'' and insert ''(d)(1)''.

Page 11, line 6, insert ''the first place it appears'' before the semicolon.

Page 14, line 25, insert '', at the sole and unreviewable discretion of the Secretary, acting through the Under Secretary for Cybersecurity and Infrastructure Protection,'' after ''subsection''.

Page 15, line 8, insert '', at the sole and unreviewable discretion of the Secretary, acting through the Under Secretary for Cybersecurity and Infrastructure Protection,'' after ''section''.

Page 15, line 21, insert ''at the sole and unreviewable discretion of the Secretary, acting through the Under Secretary for Cybersecurity and Infrastructure Protection,'' after ''Center,''.

Page 17, line 20, insert ''or exclude'' after ''remove''.

Page 17, line 23, strike ''risks'' and insert ''risk''.

Page 23, line 23, insert '', or'' before ''that''.

Page 29, line 25, strike ''paragraphs'' and insert ''subparagraphs''.

Page 30, line 15, insert ''or exclude'' after ''remove''.

Page 32, line 4, insert ''or exclude'' after ''remove''.

Page 33, line 2, insert '', except for purposes authorized in this section'' before the period at the end.

Page 34, line 16, insert ''or exclude'' after ''remove''.

Page 36, line 18, insert ''in good faith'' before ''fails''.

Page 39, beginning line 19, strike ''of the violation of any restriction specified in paragraph (3), (6), or 7(B), or any other provision of this section, that is the basis for such action'' and insert ''on which the cause of action arises''.

Page 41, strike lines 5 through 11.

Page 44, line 19, strike ''(I)'' and insert ''(J)''.

Page 44, beginning line 19, insert the following:

''(I) PROHIBITED CONDUCT.—Nothing in this section may be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.''.

Page 46, line 7, insert ''and'' before ''information''.

Page 48, lines 9 through 10, move the proposed subparagraph (H) two ems to the left.

Page 48, lines 13 through 16, move the proposed subparagraphs (K) and (L) two ems to the left.

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

The Chair recognizes the gentleman from Texas.

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

The manager's amendment to H.R. 1731 further clarifies the intent of several important provisions of the bill. These modifications were made in consultation with privacy groups, industry leaders, and both the House Intelligence Committee and House Judiciary Committee.

Among the more notable changes made are: the expansion of protections for personally identifiable information to include the ''exclusion'' of information and not just the ''removal'' of information, a modification to clarify that the use of cyber threat indicators and defensive measures is limited to the purposes authorized in the bill only, and clarifying language to say that identifying the origin of a cybersecurity threat is a valid ''cybersecurity purpose.''

Each of these changes, along with the others made in the manager's amendment, strengthen the bill and further support the committee's mission to help protect America's networks and systems from cyber attacks while, at the same time, ensuring that an individual's private information enjoys robust protection as well.

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

Mr. THOMPSON of Mississippi. Mr. Chairman, I claim the time in opposition, although I am not opposed to the amendment.

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

There was no objection.

Mr. THOMPSON of Mississippi. Mr. Chairman, the McCaul amendment makes several technical and clarifying changes to H.R. 1731 to reflect feedback from committee Democrats, Department of Homeland Security, and stakeholders.

Last week during committee consideration, the gentleman from Louisiana, Representative RICHMOND, offered an amendment to refine the 2-year statute of limitations on citizen suits against the Federal Government for privacy violations. The underlying bill requires the clock to toll from the date when the government violated the citizen's privacy. The likelihood that a citizen will know the exact date when the personal information was mishandled is pretty remote. As such, Democrats argue that the provision was tantamount to giving the Federal Government a free pass to violate the privacy protections under this act.

I am pleased to see that the gentleman from Texas, Chairman MCCAUL, has listened to Democrats' concerns and has the amendment adjust the language, though it could use further refinement.

I am also pleased that the amendment clarifies that all public utilities—not just electric utilities—are covered under this bill.

The changes to the underlying bill that this amendment would make are in line with our shared goals of bolstering cybersecurity and improving the quality of information that the private sector receives about timely cyber threats. Accordingly, I support the McCaul amendment.

I yield back the balance of my time.

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

The amendment was agreed to.

AMENDMENT NO. 2 OFFERED BY MR. RATCLIFFE

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

Mr. RATCLIFFE. Mr. Chairman, I rise as the designee of the gentleman from New York (Mr. KATKO) to offer amendment No. 2.

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 1, line 12, insert the following (and redesignate subsequent subparagraphs accordingly):

(A) by amending paragraph (2) to read as follows:

''(2) the term 'incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system;''.

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

The Chair recognizes the gentleman from Texas.

Mr. RATCLIFFE. Mr. Chairman, I rise today in support of amendment No. 2. This is a bipartisan amendment that will help clarify language in both the Homeland Security Act and this bill.

This amendment narrows the definition of the word ''incident'' to ensure that a cybersecurity incident is limited to actions taken against an information system or information stored on that system. This amendment, Mr. Chairman, ensures that information shared with the NCCIC or other private entities is limited to threats and actions against information systems and information stored on that system.

Mr. MCCAUL. Will the gentleman yield?

Mr. RATCLIFFE. I yield to the gentleman from Texas.

Mr. MCCAUL. Mr. Chairman, I support this bipartisan language that will help clarify language in both the Homeland Security Act and this bill by narrowing the definition of the word ''incident'' to ensure that a cybersecurity incident is limited to actions taken against an information system or information stored on that system.

This amendment ensures that information shared with the NCCIC or other private entities is limited to threats to and actions against information systems and information stored on that system.

I also want to thank the gentleman from California (Mr. MCCLINTOCK) for being a leader on this issue and for calling this loophole, if you will, to the attention of the committee to make this a stronger bill on this floor.

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

Mr. RICHMOND. Mr. Chairman, I claim the time in opposition, although I am not opposed to the amendment.

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

There was no objection.

Mr. RICHMOND. Mr. Chairman, I support this amendment to make an important change to a definition in the act and the law.

A strength of this bill acknowledged by some in the privacy community are the limitations that the bill places on the authorizations for sharing and network monitoring. These activities can only be carried out for a ''cybersecurity purpose.'' Among other things, this limitation is intended to ensure that information is not shared for surveillance or law enforcement purposes and the authorization for network monitoring is not exploited by an overzealous employer who wants to track his employees' every move on the Internet.

However, because of the broadness of a term within the definition of ''cybersecurity purpose,'' it came to light that the language could be interpreted far more expansively than intended.

I commend the gentleman from New York (Mr. KATKO) and the gentleman from Texas (Mr. RATCLIFFE), who is now offering the amendment, for tightening up the definition of ''incident'' in this bill and the underlying law.

We use our smartphones, tablets, and computers for all manner of things, from setting up doctor appointments to buying groceries or ordering books. It is important that, even as we seek to bolster cybersecurity, we do not lose sight of the need to protect the privacy interest of ordinary Americans. That is why I support the Ratcliffe amendment. It will ensure that, in practice, the activities undertaken in this bill are limited to protecting networks and the data on them.

I urge an ''aye'' vote on this amendment, and I yield back the balance of my time.

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

The amendment was agreed to.

AMENDMENT NO. 3 OFFERED BY MR. LANGEVIN

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

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

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

In section 2(a)(1), redesignate subparagraphs (A) and (B) as subparagraphs (B) and (C), respectively.

In section 2(a)(1), insert before subparagraph (B), as so redesignated, the following:

(A) by amending paragraph (1) to read as follows:

''(1)(A) except as provided in subparagraph (B), the term 'cybersecurity risk' means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism;

''(B) such term does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement;''.

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

The Chair recognizes the gentleman from Rhode Island.

Mr. LANGEVIN. Mr. Chairman, the amendment that I am offering makes a fine bill even better. It clarifies that the definition of ''cybersecurity risk''—and, by extension, the definition of ''cybersecurity purpose''—does not apply to actions that solely involve the violation of consumer terms of service or consumer licensing agreements.

This is a small but important change that will protect Americans' privacy and ensure that white hat security researchers are not inadvertently monitored. The cyber threat data that will help turn the tide against malicious actors are security vulnerabilities, attack vectors, and indicators of compromise. What will not help is knowing that a consumer has violated a Byzantine terms of service agreement or that a researcher is testing software for exploitable bugs that he or she will then share with the security community.

While not every terms of service violation is well-meaning or born of ignorance, there is no doubt in my mind that the existing body of contract law is more than capable of facilitating dispute resolution in these cases.

The exclusion my amendment proposes is not new to this floor. Both the 2012 and the 2013 versions of CISPA, which I worked on very closely while a member of the House Intelligence Committee, contained similar exclusions, and the Protecting Cyber Networks Act that passed the House yesterday also includes this language. The amendment also makes clear that the exclusion applies only for actions that solely violate terms of service. An action that disrupted an information system in addition to being a violation of terms of service would still constitute a cybersecurity risk.

Trust is the fundamental element of any information-sharing regime. The bill that we are considering is designed to build that trust by limiting the use of information shared to cybersecurity purposes and ensuring that indicators are scrubbed of any personal information before sharing. My amendment strengthens that trust by making it clear that our focus is on the many real cyber threats out there, not on consumers and researchers.

I would like to again express my deep thanks to the chairman of the committee, Mr. MCCAUL, for his steadfast dedication on the issue of cybersecurity, and I would like to particularly thank his staff for working with us on this amendment.

The chairman and the Democratic ranking member, Mr. THOMPSON, have done this body proud, and I certainly urge the adoption of my amendment and the underlying bill.

With that, I reserve the balance of my time.

Mr. MCCAUL. Mr. Chairman, I ask unanimous consent to claim the time in opposition, though I am not opposed to the amendment.

The CHAIR. Is there objection to the request of the gentleman from Texas?

There was no objection.

The CHAIR. The gentleman is recognized for 5 minutes.

Mr. MCCAUL. Mr. Chairman, I support this amendment, which would clarify that the term ''cybersecurity risk'' does not apply to actions solely involving violations of consumer terms of service or consumer licensing agreements.

This amendment will protect consumers from having information shared with the government due to a minor or unwitting violation of the terms of service, such as a violation of one's Apple iTunes agreement, which my teenage daughters would appreciate.

This amendment and this bill are meant to enhance the sharing of cybersecurity information within the government and the public. In order to promote voluntary sharing, the public needs to feel confident that the sole act of violating a terms of service or licensing agreement won't be shared with the NCCIC and that this bill is not a tool to enforce violations regarding terms of service or licensing agreements. These violations have robust legal remedies in place and should be handled through those channels.

I think this strengthens the bill, and I appreciate the gentleman's amendment to do so. I support this amendment.

I reserve the balance of my time.

Mr. LANGEVIN. I thank the chairman for his kind words of support.

As many in this Chamber know, Chairman MCCAUL and I have a long history on the issue of cybersecurity, from our time as co-chairs of the Commission on Cybersecurity for the 44th Presidency to our current roles as the cofounders and co-chairs of the Congressional Cybersecurity Caucus, along with a variety of other collaborations that he and I have engaged in.

□ 1015

Mr. MCCAUL. Will the gentleman yield?

Mr. LANGEVIN. I yield to the gentleman from Texas.

Mr. MCCAUL. I thank the gentleman for yielding. I would just like to highlight for all my colleagues the great work that we do in the Cybersecurity Caucus with my good friend and colleague from Rhode Island. The briefings we host every few weeks bring some of the brightest minds in both government and the private sector to the Hill to educate Members and staff on this national security issue.

When we first started the caucus in 2008, cyber was a topic very few Members knew anything about. It wasn't really cool to know about cybersecurity. We have made great progress, I believe, the gentleman and I, since that time in raising the level of debate, engagement, awareness, and education with the Members on this critical subject.

I hope that the Members and the staff will continue to take advantage of the opportunities afforded by our caucus as our lives become even more interconnected in cyberspace. I think this issue has never been more relevant and more of a threat, quite frankly, than it is today.

Mr. LANGEVIN. I thank the chairman.

I am fond of saying that cybersecurity is not a problem to be solved but a challenge to be managed. I thank the chairman for his collaboration and his leadership on this issue, along with Ranking Member THOMPSON. I certainly look forward to the caucus' continuing contributions to the discussion.

Ms. LOFGREN. Will the gentleman yield?

Mr. LANGEVIN. I yield to the gentlewoman from California.

Ms. LOFGREN. I thank the gentleman for yielding.

I would just like to thank him for his amendment. It prevents this bill from becoming like the CFAA, which treats noncriminal activity as something wrong. This and the Katko-Lofgren amendment that preceded it narrow the bill, and both deserve support. I thank the gentleman for yielding and his amendment.

Mr. LANGEVIN. I thank the gentlewoman for her comments and for her support.

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

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

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

The amendment was agreed to.

AMENDMENT NO. 4 OFFERED BY MS. JACKSON LEE

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

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

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 10, line 11, strike ''and'' at the end.

Page 10, line 16, insert ''and'' after the semicolon.

Page 10, beginning line 17, insert the following:

''(vi) remains current on industrial control system innovation; industry adoption of new technologies, and industry best practices;''.

The 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.

Ms. JACKSON LEE. Mr. Chairman, let me express my appreciation to the chairman and ranking member of the full committee. Again, they have shown the kind of leadership that the Nation needs on dealing with homeland security. My particular appreciation to the chairman and ranking member of the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, as they have worked together and presented legislation that provided a very vigorous debate in the subcommittee and the full committee.

We believe that we are making enormous leaps and bounds. We are not where we need to be, but we are making leaps and bounds on the whole question of cybersecurity.

Over the last couple of years, Mr. Chairman, even someone just reaching kindergarten understands hacking, understands the collapse that we have seen in the variety of major retail entities and banking entities, and they recognize that we have a new lingo but a new problem.

Frankly, almost maybe 10 years ago, or maybe somewhere around 7 years ago, as the infrastructure of the United States was under transportation security, we made the note that 85 percent of the Nation's cyber is in the private sector. This legislation is a real approach. The National Cybersecurity Protection Advancement Act of 2015 clearly puts the Department of Homeland Security where it needs to be and provides the National Cybersecurity and Communications Integration Center as the anchor of the information coming into the Federal Government and the vetting entity where Americans can feel that their data can be protected and our civil liberties are protected.

Mr. Chairman, my amendment deals with the industrial control systems. All of us know them. I have been to water systems and seen the impact that a cyber attack could have; the electric grid, all of these are in the eye of the storm, and they are in private hands. Attacks against industrial control systems doubled last year, according to a new report from Dell.

''We have over a million firewalls sending data to us on a minute-by-minute basis,'' said John Gordineer, director of product marketing for network security at Dell.

Gordineer said:

We anonymize the data and see interesting trends. In particular, attacks specifically targeting SCADA industrial control systems rose 100 percent in 2014 compared to the previous year—2014.

Countries most affected were Finland, the U.K., and, yes, the United States of America. The most common attack vector against these systems were buffer overflow attacks.

The underlying premise of my amendment, the public benefit of this amendment, is that taxpayer dollars provided to ensure cybersecurity of public and private computer networks will focus on real-world applications that reflect how businesses and industries function.

So I thank both my colleagues for it. This amendment, in particular, will be an important addition to the legislation, which I believe can be supported by every Member. The amendment states that the Department of Homeland Security, in carrying out the functions authorized under this bill, remain current on industrial control system innovation, industry adoption of new technologies, and industry best practices.

Industrial control systems are rarely thought of as long as they work as designed. Industrial control systems are used to deliver utility services to homes and businesses, add precision and speed to manufacturing, and process our foods into finished products. Industrial control systems are responsible for the lights that brighten our cities; for the clean drinking water, which I indicated many of us visited these systems; of the sewage; of automobiles that travel our highways; and the rows upon rows of foods that fill our shelves at grocery stores.

We only need to look recently at a contamination of ice cream across the Nation to know that industrial control systems are extremely important. They are also used in large-scale manufacturing. A day does not pass in this country when citizens' lives are not impacted.

So, Mr. Chairman, I am asking my colleagues to recognize that we are in control, but the industrial control systems may, in fact, control our daily lives. My amendment is asking that the Department of Homeland Security, in carrying out its function authorized under this bill, remain current on industrial control system innovation, industry adoption of new technologies, and industry best practices.

I ask my colleagues, as I ask to put my entire statement into the RECORD—it lists a whole litany of the private sector infrastructure dealing with industrial control. I am hoping that my amendment will be passed in order to ensure that all aspects of our cyber world are protected for the American people.

Mr. Chair, I thank Chairman MCCAUL and Ranking Member THOMPSON for their bipartisanship in bringing H.R. 1731, the ''National Cybersecurity Protection Advancement Act of 2015'' before the House for consideration.

As a senior member of the House Committee on Homeland Security, I am dedicated to protecting our nation from threats posed by terrorists or others who would wish to do our Nation harm.

This is the first of 3 Jackson Lee amendments that will be considered for H.R. 1731, the ''National Cybersecurity Protection Advancement Act of 2015.''

Jackson Lee Amendment No. 4 is simple and will be an important addition to the legislation, which I believe can be supported by every Member of the House.

The Jackson Lee amendment states that the Department of Homeland Security, in carrying out the functions authorized under this bill, will remain current on industrial control system innovation, industry adoption of new technologies, and industry best practices.

Industrial control systems are rarely thought of as long as they work as designed.

Industrial control systems are used to: deliver utility services to homes and businesses; add precision and speed to manufacturing; and process raw foods into finished products.

Industrial control systems are responsible for the lights that brighten our cities at night; the clean drinking water that flows from faucets in our homes; automobiles that travel our highways; and the rows upon rows of foods that fill the shelves of grocery stores.

Industrial control systems are also used in large-scale manufacturing of home appliances, medicines, and products large and small that are found in our homes and offices.

A day does not pass in this country when citizens' lives are not touched by the output of industrial control systems.

The critical importance electricity; water, natural gas, and other utility services are all provided by industrial control systems.

Industrial control systems help keep the cost of everyday consumer products low, and they are essential to meeting consumer demand for goods and services.

Industrial control systems undergo constant improvements as owners and operators work to address vulnerabilities and improve efficiency.

Innovation is occurring rapidly in industrial control systems.

All industrial control systems have one thing in common—they require computer software, firmware, and hardware.

In its wisdom, the Committee on Homeland Security incorporated industrial control systems in its cybersecurity legislation, because industrial control systems are vulnerable to computer errors, accidents, and cybersecurity threats.

Coupled with the cybersecurity challenges of industrial control systems is the rapid pace of innovation.

For example, a new innovation being adopted by industrial control systems involves 3-Dimential or 3–D printing.

3–D printing involves scanning a physical object with a printer made of a high-power laser that fuses small particles of plastic, metal, ceramic, or glass powders into the object's size and shape.

According to PricewaterhouseCoopers, the 3–D printing of jet engine parts to coffee mugs is possible.

3–D printing has the potential to shrink supply chains, save product development times, and increase customization of products.

3–D printing is not the only innovation that will impact industrial control systems.

Electricity delivery depends on industrial control systems.

The biggest innovation in electricity delivery is the smart grid, which is quickly replacing old electricity delivery and metering technology in cities across the Nation.

The term "smart grid" encompasses a host of inter-related technologies rapidly moving into public use to reduce or better manage electricity consumption.

Smart grid systems can aid electricity service providers, users, or third-party electricity usage management service providers to monitor and control electricity use.

The smart grid is also making it possible to more efficiently manage the flow of electricity to residential and industrial consumers.

Electric utility meters that were once read once a month are being replaced by smart meters that can be read remotely using smart grid communication systems every 15 minutes or less.

The smart grid is capable of monitoring the consumption of electricity down to the individual residential or commercial property.

DHS should remain current as innovations like 3–D printing and smart grid technologies are introduced to industrial control systems.

This Jackson Lee amendment is a good contribution to H.R. 1731.

I request support of this amendment by my colleagues on both sides of the aisle.

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

Mr. MCCAUL. Mr. Chairman, I ask unanimous consent to claim the time in opposition, though I am not opposed to the amendment.

The CHAIR. Is there objection to the request of the gentleman from Texas?

There was no objection.

The CHAIR. The gentleman is recognized for 5 minutes.

Mr. MCCAUL. Mr. Chairman, I support this amendment, which will modify the Information Sharing Structure and Processes section of the bill relating to the National Cybersecurity and Communications Integration Center's, or NCCIC's, Industrial Control System.

The Cyber Emergency Response Team, ICS-CERT. This amendment directs the ICS-CERT to remain current on ICS innovation, industry adoption of new technologies, and industry best practices. This amendment directs the ICS-CERT to keep abreast of new, innovative technologies. This will enable the ICS-CERT to respond, when requested, with the latest and most current technologies and practices.

It is a good amendment. I thank the gentlewoman for bringing it. I urge my colleagues to support this amendment, and I yield back the balance of my time.

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

The amendment was agreed to.

AMENDMENT NO. 5 OFFERED BY MR. CASTRO OF TEXAS

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

Mr. CASTRO of Texas. Mr. Chairman, I have an amendment at the desk.

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 11, line 22, insert before the semicolon at the end the following: '', and, to the extent practicable, make self-assessment tools available to such businesses to determine their levels of prevention of cybersecurity risks''.

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

The Chair recognizes the gentleman from Texas.

Mr. CASTRO of Texas. Mr. Chairman, first, I would like to thank my colleague and fellow Texan, Chairman MCCAUL, and Ranking Member BENNIE THOMPSON of the House Homeland Security Committee for bringing up my amendment for consideration to H.R. 1731.

This amendment supports small businesses across the Nation at no cost to taxpayers. My amendment would make self-assessment tools available to small- and medium-sized businesses so they can determine their level of cybersecurity readiness. Oftentimes, medium-sized and small businesses don't have the framework or capability in place to protect against cybersecurity threats. In 2014, for example, 31 percent of all cyber attacks were directed not at large businesses but at businesses with less than 250 employees. This is a 4 percent increase from 2013.

As the chairman knows, Texas is home to many small companies in so many critical industries: biomed and pharmaceuticals, energy, manufacturing, and many more. Some of these businesses employ as few as 5 to 10 people, and their technology is unprotected, vulnerable to cyber attacks.

Today most small businesses use the Internet, collect customers' information, and store sensitive information on business computers. Yet many of these same companies don't have the readily available information to self-assess their ability to defend their digital assets. They lack the tools necessary for determining cybersecurity readiness.

This pro-small business amendment fills that void and provides the information and tools needed to secure and empower small businesses across the country.

Mr. Chairman, I yield 1 minute to the gentleman from Louisiana (Mr. RICHMOND).

Mr. RICHMOND. Mr. Chairman, I rise to support the amendment offered by the gentleman from Texas (Mr. CASTRO). Over the course of the past year, cyber breaches at Target, Sony, eBay, and Anthem have consumed headlines and brought awareness to the vulnerability of large corporations to cyber threats.

Although cyber attacks against small businesses are not well-publicized, they are a dangerous threat that we cannot afford to ignore. In fact, in 2012 alone, the National Cyber Security Alliance found that 60 percent of small businesses shut down within 6 months of a data breach. Small businesses are attractive prey for hackers because they often lack the resources necessary to identify cyber vulnerabilities and harden their cyber infrastructure.

Mr. CASTRO's amendment builds upon language I inserted into the underlying bill that is aimed at improving cybersecurity capabilities of small businesses.

Mr. Chairman, I urge my colleagues to help protect small businesses from cyber threats by supporting this important amendment.

Mr. CASTRO of Texas. Thank you, Congressman RICHMOND, for reminding us that the big businesses that get attacked by hacks make the big headlines, but we can't forget about small businesses and medium-sized businesses who day in and day out are vulnerable to the same kind of cybersecurity threats.

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

Mr. MCCAUL. Mr. Chairman, I ask unanimous consent to claim the time in opposition, though I am not opposed to the amendment.

The CHAIR. Is there objection to the request of the gentleman from Texas?

There was no objection.

The CHAIR. The gentleman is recognized for 5 minutes.

Mr. MCCAUL. Mr. Chairman, I support the gentleman's amendment. The gentleman is correct. Small- and medium-sized businesses are the lifeblood of our economy, yet they often cannot dedicate the resources to address cybersecurity issues. Making self-assessment tools available to these businesses will allow them to determine their levels of cyber risk and manage the risk through appropriate prevention.

I urge my colleagues to support this amendment, Mr. Chairman, and I yield back the balance of my time.

Mr. CASTRO of Texas. Mr. Chairman, I yield back back the balance of my time.

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

The amendment was agreed to.

AMENDMENT NO. 6 OFFERED BY MR. CASTRO OF TEXAS

The CHAIR. It is now in order to consider amendment No. 6 printed in part B of House Report 114–88.

Mr. CASTRO of Texas. Mr. Chairman, I have an amendment at the desk.

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Page 52, beginning line 12, insert the following:

"SEC. 232. NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM.

''(a) IN GENERAL.—The Secretary may establish a consortium to be known as the 'National Cybersecurity Preparedness Consortium' (in this section referred to as the 'Consortium').

''(b) FUNCTIONS.—The Consortium may—

''(1) provide training to State and local first responders and officials specifically for preparing and responding to cyber attacks;

''(2) develop and update a curriculum utilizing the National Protection and Programs Directorate of the Department sponsored Community Cyber Security Maturity Model (CCSMM) for State and local first responders and officials;

''(3) provide technical assistance services to build and sustain capabilities in support of cybersecurity preparedness and response;

''(4) conduct cybersecurity training and simulation exercises to defend from and respond to cyber-attacks;

''(5) coordinate with the National Cybersecurity and Communications Integration Center to help States and communities develop cybersecurity information sharing programs; and

''(6) coordinate with the National Domestic Preparedness Consortium to incorporate cybersecurity emergency responses into existing State and local emergency management functions.

''(c) MEMBERS.—The Consortium shall consist of academic, nonprofit, and government partners that develop, update, and deliver cybersecurity training in support of homeland security. Members shall have prior experience conducting cybersecurity training and exercises for State and local entities.''.

Page 52, before line 17, insert the following:

''Sec. 232. National Cybersecurity Preparedness Consortium.''.

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

The Chair recognizes the gentleman from Texas.

Mr. CASTRO of Texas. Mr. Chairman, first, I am very honored to be joined by my fellow colleagues and Members of Congress from both parties from San Antonio, Texas—Congressmen SMITH, DOGGETT, CUELLAR, and HURD—who each represent a portion of Bexar County and have joined me on this amendment.

My amendment would give the Secretary of Homeland Security authority to establish the National Cybersecurity Preparedness Consortium, or NCPC, within the Department of Homeland Security. Doing so would formally allow this consortium, which already exists outside of the government, to assist State and local entities in developing their own viable and sustainable cybersecurity programs, and it would be at no cost to taxpayers.

The NCPC consists of five university partners. The University of Texas at San Antonio leads the effort, along with Texas A&M University in College Station, the University of Arkansas, the University of Memphis, and Norwich University in Vermont.

□ 1030

These schools proactively came together to coordinate their work, helping State and local officials prepare for cyber attacks. The consortium also develops and carries out trainings and exercises to increase cybersecurity knowledge.

Additionally, the NCPC uses competitions and workshops to encourage more people to pursue careers in cybersecurity and grow the industry's workforce.

States and communities need the ability to prevent, detect, respond to, and recover from cyber events as they would any other disaster or emergency situation, and they need to be aware of the fact that cyber events could impede emergency responders' ability to do their jobs.

This amendment helps address those State and local needs by codifying this valuable consortium.

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

Mr. MCCAUL. Mr. Chairman, I ask unanimous consent to claim the time in opposition, although I am not opposed to the amendment.

The CHAIR. Is there objection to the request of the gentleman from Texas?

There was no objection.

The CHAIR. The gentleman is recognized for 5 minutes.

Mr. MCCAUL. Mr. Chairman, I support this amendment, which establishes the National Cybersecurity Preparedness Consortium, consisting of university partners and other stakeholders who proactively coordinate to assist State and local officials in cybersecurity preparation and the prevention of cyber attacks.

The amendment directs the Cybersecurity and Infrastructure Protection Directorate to update curriculum for first responders, provide technical assistance where possible, and conduct simulations and other training to help State and local officials be better prepared for cyber attacks.

The amendment directs the consortium to consist of academic, nonprofit, and government partners to deliver the best training possible, which will further advance the overall goal of H.R. 1731, to strengthen the resiliency of Federal and private networks and, thus, protect the data of the American people more effectively.

I am a strong proponent of this type of consortium. I am pleased that the gentleman from Texas brought this amendment. I urge my colleagues to support the amendment.

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

Mr. CASTRO of Texas. Mr. Chairman, I yield back the balance of my time.

Mr. MCCAUL. Mr. Chairman, I yield such time as he may consume to the gentleman from Texas (Mr. HURD).

Mr. HURD of Texas. Mr. Chairman, I thank the chairman for his work in making this amendment happen. I urge my colleagues to support this amendment to H.R. 1731.

Cybersecurity is not just a buzzword. Oftentimes, large governments and governments have plans in place to mitigate and respond to cyber threats, but many smaller State and local entities do not. This is why I cosponsored and stand in support of Representative CASTRO's amendment to H.R. 1731.

Five leading universities across the Nation have teamed up to face these cyber issues head on, including the University of Texas at San Antonio and my alma mater, Texas A&M University.

The proposed consortium would provide valuable training to local and first responders in the event of a catastrophic cyber attack. It would also provide technical assistance services to build and sustain capabilities in support of cybersecurity preparedness and response, and it would coordinate with other crucial entities, such as the Multi-State Information Sharing and Analysis Center and NCCIC.

It is clear that we must focus on cyber preparedness not only at the Federal level, but the local level as well.

Again, this is why I urge my colleagues to support this.

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

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

The amendment was agreed to.

AMENDMENT NO. 7 OFFERED BY MR. HURD OF TEXAS

The CHAIR. It is now in order to consider amendment No. 7 printed in part B of House Report 114–88.

Mr. HURD of Texas. Mr. Chairman, I have an amendment at the desk.

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Add at the end the following:

SEC. ___. PROTECTION OF FEDERAL INFORMATION SYSTEMS.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended by adding at the end the following new section:

''SEC. 233. AVAILABLE PROTECTION OF FEDERAL INFORMATION SYSTEMS.

''(a) IN GENERAL.—The Secretary shall deploy and operate, to make available for use by any Federal agency, with or without reimbursement, capabilities to protect Federal agency information and information systems, including technologies to continuously diagnose, detect, prevent, and mitigate against cybersecurity risks (as such term is defined in the second section 226) involving Federal agency information or information systems.

''(b) ACTIVITIES.—In carrying out this section, the Secretary may—

''(1) access, and Federal agency heads may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information traveling to or from or stored on a Federal agency information system, regardless of from where the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or prevent Federal agency heads from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);

''(2) enter into contracts or other agreements, or otherwise request and obtain the assistance of, private entities to deploy and operate technologies in accordance with subsection (a); and

''(3) retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect Federal agency information and information systems from cybersecurity risks, or, with the approval of the Attorney General and if disclosure of such information is not otherwise prohibited by law, to law enforcement

only to investigate, prosecute, disrupt, or otherwise respond to—

''(A) a violation of section 1030 of title 18, United States Code;

''(B) an imminent threat of death or serious bodily harm;

''(C) a serious threat to a minor, including sexual exploitation or threats to physical safety; or

''(D) an attempt, or conspiracy, to commit an offense described in any of subparagraphs (A) through (C).

''(c) CONDITIONS.—Contracts or other agreements under subsection (b)(2) shall include appropriate provisions barring—

''(1) the disclosure of information to any entity other than the Department or the Federal agency disclosing information in accordance with subsection (b)(1) that can be used to identify specific persons and is reasonably believed to be unrelated to a cybersecurity risk; and

''(2) the use of any information to which such private entity gains access in accordance with this section for any purpose other than to protect Federal agency information and information systems against cybersecurity risks or to administer any such contract or other agreement.

''(d) LIMITATION.—No cause of action shall lie against a private entity for assistance provided to the Secretary in accordance with this section and a contract or agreement under subsection (b)(2).''.

(b) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 226 (relating to cybersecurity recruitment and retention) the following new item:

''Sec. 233. Available protection of Federal information systems.''.

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

The Chair recognizes the gentleman from Texas.

Mr. HURD of Texas. Mr. Chairman, every day and every hour, hacktivists and state actors are attempting to breach U.S. Government systems.

This is an ongoing problem I dealt with during my time at the CIA, and, since I have left, it has only gotten worse. They are attempting to steal valuable information that could be used against us.

The EINSTEIN Program is a valuable tool that the U.S. Government can deploy to respond to and mitigate cyber threats. The EINSTEIN Program was intended to provide DHS a situational awareness snapshot of the health of the Federal Government's cyberspace.

Based upon agreements with participating Federal agencies, DHS installed systems at their Internet access points to collect network flow data.

EINSTEIN 3A is the third and newest version of the program. This groundbreaking technology uses classified and unclassified information to block cyber espionage and attacks. E3A is allowing the Department of Homeland Security to paint a wider and more intelligent picture of the overall cyber threat landscape within the Federal Government, enabling strong correlation of events and the ability to provide early warning and greater context about emerging risks.

Cutting-edge programs such as EINSTEIN can serve as a groundbreaking tool to stop criminals, hacktivists, and nation-states from harming the American public and government.

I urge my colleagues to support codifying the E3A program and vote in favor of this amendment.

Mr. MCCAUL. Will the gentleman yield?

Mr. HURD of Texas. I yield to the gentleman from Texas.

Mr. MCCAUL. I support this amendment, which would authorize and codify the current EINSTEIN Program operated in the Department of Homeland Security.

The EINSTEIN Program, as deployed, makes available the capability to protect Federal agency information and information systems. The Einstein Program includes technologies to diagnose, detect, prevent, and mitigate cybersecurity risks involving Federal information systems.

I would also like to thank my colleague and fellow chairman, Mr. CHAFFETZ, of the Oversight and Government Reform Committee for working with the Committee on Homeland Security on this important issue.

Mr. HURD of Texas. Mr. Chairman, I reserve the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Chair, I claim the time in opposition, although I am not in opposition to the amendment.

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

There was no objection.

Mr. THOMPSON of Mississippi. Mr. Chairman, this amendment would authorize the Department of Homeland Security's program to provide web-based security services to U.S. Federal civilian agencies.

The program is known as EINSTEIN. When fully implemented, it is expected to provide all participating Federal agencies with the ability to know the cyber threats they face and protect their systems from insider and outsider threats.

To fully implement EINSTEIN to protect Federal civilian networks, there are complex interagency privacy and coordination issues that still need to be settled.

This authorization should help the Department of Homeland Security's efforts at closing out those issues as it confers specific statutory authority to the Department to pursue EINSTEIN.

I support the amendment, and I urge my colleagues to vote ''aye.''

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

Mr. HURD of Texas. Mr. Chairman, I yield back the balance of my time.

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

The amendment was agreed to.

AMENDMENT NO. 8 OFFERED BY MR. MULVANEY

The CHAIR. It is now in order to consider amendment No. 8 printed in part B of House Report 114–88.

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

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Add at the end the following new section:

SEC. ___. 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 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. Mr. Chairman, I thank the chairman for the opportunity to present this amendment, very similar, Mr. Chairman, to the amendment that I presented yesterday that was approved by a majority of both Republicans and Democrats. It is a 7-year sunset provision to the bill.

Here again, today, we are dealing with two very real and very serious concerns, security of our people and the freedoms and liberties of our people. We are called upon to do that very often here in Congress. Sometimes, we get those balances exactly right, and sometimes, we don't.

Sometimes, we err too much on the side of safety and protection and security to the expense of our individual liberties. Other times, we err on the other side and do not provide the requisite level of safety and security that the citizens rightly demand of Congress.

All this bill does is force us to make sure that we keep an eye on this piece of legislation to make sure that we got the balance exactly right. I know that many folks will say: Well, you know, Mr. MULVANEY, we have the opportunity at any time to go back in and fix the bill.

I know that, and we have done that from time to time, but, by the same token, this is a very busy place, and a lot of bills tend to fall between the cracks.

Putting in a hardwired 7-year sunset into this piece of legislation will force us not only to keep an eye on this on an ongoing basis, but to come here 7 years from now and make sure that we have done it precisely correctly.

I think it is the exact right approach. In fact, I have often wished that we put sunset provisions, Mr. Chairman, in every single piece of legislation that we have, but we don't have that opportunity here today.

We do have the opportunity to put a sunset into this very important piece of legislation, and I hope that the House does the same thing today as it did yesterday and approve this amendment by an overwhelming margin.

Mr. MCCAUL. Will the gentleman yield?

Mr. MULVANEY. I yield to the gentleman from Texas.

Mr. MCCAUL. As an advocate for civil liberties and privacy rights, I did

not oppose the inclusion of his amendment here today on the floor, and that was for good reason.

I believe that we need an open and fair debate on this measure, this amendment. We need transparency in the process here on the floor. My committee has undertaken that since day one as we assembled this bill in a bipartisan fashion.

While, normally, I do support sunset provisions, I think, in this case, submitting a sunset provision to this vital national security program would not be in our best interest.

I have heard, time and time again, from industry and other stakeholders that a sunset would stifle the sharing of this valuable cyber threat information. It would undermine everything that we are trying to do here today as we try to incentivize participation and investment in this voluntary program.

While I do have tremendous respect for the gentleman and his point of view on this, I will vote ''no'' and oppose this amendment.

Mr. MULVANEY. Mr. Chairman, I applaud the chairman for doing something that doesn't happen nearly enough in this Chamber. He is allowing an amendment to come to the floor that he opposes.

I think that doesn't happen nearly enough here. I think it speaks volumes to some of the recent steps we have taken to improve Member participation in the process, and I think we will be better as an institution for it.

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

Mr. THOMPSON of Mississippi. Mr. Chairman, I claim the time in opposition, although I am not in opposition to the amendment.

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

There was no objection.

Mr. THOMPSON of Mississippi. Mr. Chairman, I appreciate, as I said, the maker of this amendment.

Let me be clear, I offered the very same amendment in markup. It failed on a party-line vote, and this is democracy; but a little thing that concerns me is that, when we went to the Rules Committee, my chairman gave an indication that he really didn't have a problem with the 7-year sunset.

Mr. MCCAUL. Will the gentleman yield on that point?

Mr. THOMPSON of Mississippi. I yield to the gentleman from Texas, my chairman.

Mr. MCCAUL. Again, I just want to clarify what I believe to be the record, and that was I was not opposed to this amendment going to the floor for a full and fair debate.

I respect the gentleman's interpretation of that. I simply was not opposed to this going to the floor, and I think it deserves a full debate, as we saw yesterday as well.

Mr. THOMPSON of Mississippi. Thank you.

Mr. Chairman, I will read for the RECORD the statement my chairman made in Rules. Mr. MCCAUL said:

There is an amendment that has a 7-year sunset provision, and I will be honest, I will not oppose that. I think 7 years is ample time to advance those relationships and while, at the same time, giving Congress the authority to reauthorize after a 7-year period.

Mr. MCCAUL. Will the gentleman yield again?

Mr. THOMPSON of Mississippi. I yield to the gentleman from Texas.

Mr. MCCAUL. I must say that, obviously, since the time the Rules Committee discharged the amendment, there has been tremendous opposition from industry, which concerns me, about the participation in this program and the success of this program if the sunset provision is allowed to go forward, just to clarify my point of view.

□ 1045

Mr. THOMPSON of Mississippi. Mr. Chairman, reclaiming my time, I accept the gentleman's reinterpretation of the statement, and we will go forward.

Let me just say that, yesterday, on a 7-year sunset on an Intelligence bill, the House resoundingly voted for this very same amendment, 313–110. It is clear that the congressional intent is, within 7 years, that it should have been ample time for this bill to be law and now set a record for us to come back as Members of Congress and do our oversight responsibility.

Mr. Chairman, I am in strong support of Mr. MULVANEY's amendment. It is common sense.

I yield back the balance of my time.

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

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

The amendment was agreed to.

AMENDMENT NO. 9 OFFERED BY MS. HAHN

The CHAIR. It is now in order to consider amendment No. 9 printed in part B of House Report 114–88.

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

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Add the end the following:

SEC. ___. REPORT ON CYBERSECURITY VULNERABILITIES OF UNITED STATES PORTS.

Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science and Transportation of the Senate a report on cybersecurity vulnerabilities for the ten United States ports that the Secretary determines are at greatest risk of a cybersecurity incident and provide recommendations to mitigate such vulnerabilities.

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

The Chair recognizes the gentlewoman from California.

Ms. HAHN. Mr. Chairman, I thank Chairman MCCAUL and Ranking Member THOMPSON for allowing me to offer this amendment.

I rise to offer a National Cybersecurity Protection Advancement Act amendment, one to increase cybersecurity at our Nation's most at-risk ports.

This amendment will direct the Secretary of Homeland Security to submit a report to Congress assessing risks and providing recommendations regarding cybersecurity at America's most at-risk ports, such as Los Angeles, Long Beach, Oakland, New York, Houston.

According to the American Association of Port Authorities, our ports contribute $4.6 trillion to the U.S. economy, making their security critical to our Nation.

In order to remain efficient and globally competitive, our ports have become increasingly reliant on complex computer networks for everyday management. However, The Brookings Institution has found that there is a cybersecurity gap at our Nation's ports. Currently, we do not have cybersecurity standards for our ports to give Federal agencies the authority to address cybersecurity issues.

This is completely unacceptable. The threat of cyber attack on the networks that manage the flow of U.S. commerce at our ports is real.

As the Representative of the Nation's busiest port complex and as cofounder of the Congressional Ports Caucus, I know that a significant disruption at our ports cripples our economy. An estimated $1 billion a day was lost during the lockout at the Ports of Los Angeles and Long Beach back in 2002. Imagine the possible damage of a more severe disruption. For example, if our ports were targeted and hacked and unable to operate, it could cost our Nation billions and billions of dollars.

While the Port of Los Angeles is a participant in the FBI's Cyberhood Watch program and has an award-winning cybersecurity operations center, we need to ensure that all of our ports have the same ability to protect themselves from cyber attacks. This is why I have offered this amendment that addresses the lack of cybersecurity standards and safeguards at our ports.

We have ignored the cybersecurity of the networks managing our ports long enough, and it is pointless and ironic for government to continue awarding funds that are spent on the installation of new technologies if the networks they are on remain vulnerable to cyber attacks. This amendment adds no new cost to this legislation, but it will offer great security to our Nation's movement of goods.

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

Mr. RATCLIFFE. Mr. Chairman, I ask unanimous consent to claim the time in opposition, although I am not opposed to the amendment.

The CHAIR. Is there objection to the request of the gentleman from Texas?

There was no objection.

The CHAIR. The gentleman is recognized for 5 minutes.

Mr. RATCLIFFE. Mr. Chairman, I support this amendment, which requires the Department of Homeland Security to identify and mitigate cybersecurity threats to our Nation's seaports. It requires the Secretary to identify the 10 ports with the highest vulnerability to cybersecurity incidents and to fully evaluate and establish procedures to mitigate relevant cyber vulnerabilities.

America's seaports are critical infrastructure, and 95 percent of America's foreign trade travels through these seaports. A cybersecurity incident which impacts a major U.S. port could have profound effects on the global economy. The Department of Homeland Security must take immediate, proactive measures to identify and mitigate cybersecurity threats in America's most vulnerable ports.

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

Ms. HAHN. I thank you for your support, and I applaud you and the committee for working in this bipartisan manner. I urge all of my colleagues to support this amendment.

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

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

The amendment was agreed to.

AMENDMENT NO. 10 OFFERED BY MS. JACKSON LEE

The CHAIR. It is now in order to consider amendment No. 10 printed in part B of House Report 114–88.

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

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Add at the end the following:

SEC. ___. GAO REPORT ON IMPACT PRIVACY AND CIVIL LIBERTIES.

Not later than 60 months after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate an assessment on the impact on privacy and civil liberties limited to the work of the National Cybersecurity and Communications Integration Center.

The 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.

Ms. JACKSON LEE. Mr. Chairman, let me thank Mr. THOMPSON and Mr. MCCAUL for their leadership and Mr. RATCLIFFE and Mr. RICHMOND for their leadership and for the importance of this legislation on the floor today and—this is something that I have often said—for the importance of the Department of Homeland Security's being the front armor, if you will, for domestic security, and this is a very important component of domestic security.

The Jackson Lee-Polis amendment states that not later than 60 months after the date of this act the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and to the Committee on Homeland Security and Governmental Affairs of the Senate an assessment on the impact of privacy and civil liberties, limited to the work of the National Cybersecurity and Communications Integration Center.

The public benefit of this amendment is that it will provide public assurance from a reliable and trustworthy source that their privacy and civil liberties are not being compromised. Whether it is the PATRIOT Act or the USA FREEDOM Act that is now proposed, the American people understand their security, but they understand their privacy and their civil liberties. The intent of this report is to provide Congress with information regarding the effectiveness of protecting the privacy of Americans.

We have gone through too much—we have been through too much hacking, and we have lost too much personal data from a number of retail entities and elsewhere—for the American people not to be protected. This amendment will result in the sole external report on the privacy and civil liberties' impact of the programs created under this bill.

I ask that my colleagues support the Jackson Lee-Polis amendment, and I reserve the balance of my time.

Mr. MCCAUL. Mr. Chairman, I ask unanimous consent to claim the time in opposition, although I am not opposed to the amendment.

The CHAIR. Is there objection to the request of the gentleman from Texas?

There was no objection.

The CHAIR. The gentleman is recognized for 5 minutes.

Mr. MCCAUL. Mr. Chairman, I support this amendment.

The report required by this amendment would provide a quantifiable tool for the transparency, accountability, and oversight of Americans' civil liberties, and it will address privacy concerns.

Privacy is a hallmark of H.R. 1731, and any opportunity to highlight to the American people how well DHS is protecting their civil liberties, while strengthening the cyber resilience of our Federal and non-Federal networks, is a welcome endeavor.

The report will provide data on how well the program is working, and it will potentially identify any areas of improvement, which will further strengthen the robustness of DHS' cyber information-sharing practices.

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

Ms. JACKSON LEE. I thank the chair for his comments.

Mr. Chairman, privacy is of great concern to the American public in a digital economy where personal information is one of the most valuable assets of successful online business. Again, I ask for support of the Jackson Lee-Polis amendment.

Mr. Chair, I offer my thanks to Chairman MCCAUL, and Ranking Member THOMPSON for their leadership and work on H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015 to the floor for consideration.

The bipartisan work done by the House Committee on Homeland Security brought before the House this opportunity to defend our Nation against cyber threats.

I thank Congressman POLIS for joining me in sponsoring this amendment.

The Jackson Lee-Polis amendment to H.R. 1731 is simple and would improve the bill.

The Jackson Lee-Polis amendment states that, not later than 60 months after the date of this act, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Government Affairs of the Senate an assessment on the impact of privacy and civil liberties limited to the work of the National Cybersecurity and Communications Integration Center.

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 in a digital economy where personal information is one of the most valuable assets of successful online businesses.

Having detailed information on consumers allows companies to better tailor services and products to meet the needs of consumers.

Instead of relying on surveys to try to determine what consumers want, companies know what they want through their online and increasingly offline activities that are recorded and analyzed.

In 2014, a report on consumers' views of 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.

91% of adults in the survey believe that consumers have lost control over how personal information is collected and used by companies.

88% of adults believe that it would be very difficult to remove inaccurate information about them online.

80% of those who use social networking sites believe they are concerned about third parties accessing their data.

70% of social networking site users have some concerns about the government accessing some of the information they share on social networking sites without their knowledge.

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.

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

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

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

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

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

AMENDMENT NO. 11 OFFERED BY MS. JACKSON LEE

The CHAIR. It is now in order to consider amendment No. 11 printed in part B of House Report 114–88.

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

The CHAIR. The Clerk will designate the amendment.

The text of the amendment is as follows:

Add at the end the following:

SEC. ___. REPORT ON CYBERSECURITY AND CRITICAL INFRASTRUCTURE.

The Secretary of Homeland Security may consult with sector specific agencies, businesses, and stakeholders to produce and submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on how best to align federally-funded cybersecurity research and development activities with private sector efforts to protect privacy and civil liberties while assuring security and resilience of the Nation's critical infrastructure, including—

(1) promoting research and development to enable the secure and resilient design and construction of critical infrastructure and more secure accompanying cyber technology;

(2) enhancing modeling capabilities to determine potential impacts on critical infrastructure of incidents or threat scenarios, and cascading effects on other sectors; and

(3) facilitating initiatives to incentivize cybersecurity investments and the adoption of critical infrastructure design features that strengthen cybersesecurity and resilience.

The 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.

Ms. JACKSON LEE. This is a comprehensive approach, Mr. Chairman, to the issue of cybersecurity and national cybersecurity protection.

The amendment that I am offering now states that the Secretary of Homeland Security may consult with sector-specific agencies, businesses, and stakeholders to produce and submit to the Committee on Homeland Security of the House of Representatives and to the Committee on Homeland Security and Governmental Affairs of the Senate a report on how best to align federally funded cybersecurity research and development activities with private sector efforts to protect privacy and civil liberties while assuring the security and resilience of the Nation's critical infrastructure.

Again, I can recount the incidences that have brought this issue to the attention of the American people. Certainly, one of the most striking were the actions of Mr. Snowden's, so it is important that we develop research that really blocks those who would intend to do wrong, or ill, to the American people.

The amendment includes a cybersecurity research and development objective to enable the secure and resilient design and construction of critical infrastructure and more secure accompanying cyber technology. We want it to be impenetrable. We want to have a firewall that stands as a firewall. I believe that we have the capacity to have the R&D to do so.

The public benefit of this amendment is that it will make sure, as innovations occur in the private sector that can improve privacy and civil liberties protections, that they will be adopted by DHS for its programs established by this bill.

Mr. Chairman, I ask for support of the Jackson Lee amendment, and I reserve the balance of my time.

Mr. MCCAUL. Mr. Chairman, I ask unanimous consent to claim the time in opposition, although I am not opposed to the amendment.

The CHAIR. Is there objection to the request of the gentleman from Texas?

There was no objection.

The CHAIR. The gentleman is recognized for 5 minutes.

Mr. MCCAUL. Mr. Chairman, I support this enhancement that allows the Secretary of Homeland Security to consult with stakeholders and to submit a report on how best to align federally funded cybersecurity research and development activities with private sector efforts to protect privacy and civil liberties, while assuring the security and resilience of the Nation's critical infrastructure.

The promotion of research and development activities to design resilient critical infrastructure that includes cyber threat infrastructure and that also includes cyber threat consideration in its plan is important as we build the fences against the cascading effect of cyber attacks on critical infrastructures.

Again, I want to thank the gentlewoman for bringing this amendment, and I urge my colleagues to support it.

I yield back the balance of my time.

Ms. JACKSON LEE. I thank the gentleman from Texas.

Mr. Chairman, again, the American people deserve the kind of investigatory work that results in R&D that provides the kind of armor against the attacks that we have noted are possible and have occurred. With that, I ask for the support of the Jackson Lee amendment.

Mr. Chair, I offer my thanks to Chairman MCCAUL, and Ranking Member THOMPSON for their leadership and work on H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015.

This is the final of three Jackson Lee amendments offered to this legislation.

The Jackson Lee-Polis amendment to H.R. 1731 is simple and would improve the bill.

The amendment states that the Secretary of Homeland Security may consult with sector-specific agencies, businesses, and stakeholders to produce and submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on how best to align federally funded cybersecurity research and development activities with private sector efforts to protect privacy and civil liberties, while assuring the security and resilience of the Nation's critical infrastructure.

The amendment includes a cybersecurity research and development objective to enable the secure and resilient design and construction of critical infrastructure and more secure accompanying cyber technology.

Finally, this Jackson Lee amendment would support investigation into enhanced computer-aided modeling capabilities to determine potential impacts on critical infrastructure of incidents or threat scenarios and cascading effects on other sectors and facilitating initiatives to incentivize cybersecurity investments and the adoption of critical infrastructure design features that strengthen cybersecurity and resilience.

The ability to stay current and at the leading edge of innovation in the fast-moving world of computing technology will be a challenge, but one that the Department of Homeland Security can meet.

The Jackson Lee amendment lays the foundation for an array of collaborative efforts centered on learning as much as possible about critical infrastructure operations and technologies, then using that knowledge to discover how best to defend against cyber-based threats.

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

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

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

The amendment was agreed to.

AMENDMENT NO. 10 OFFERED BY MS. JACKSON LEE

The CHAIR. Pursuant to clause 6 of rule XVIII, the unfinished business is the demand for a recorded vote on the amendment offered by the gentlewoman from Texas (Ms. JACKSON LEE) on which further proceedings were postponed and on which the ayes prevailed by voice vote.

The Clerk will redesignate the amendment.

The Clerk redesignated the amendment.

RECORDED VOTE

The CHAIR. A recorded vote has been demanded.

A recorded vote was ordered.

The vote was taken by electronic device, and there were—ayes 405, noes 8, not voting 18, as follows:

[Roll No. 171]

AYES—405

Abraham	Allen	Babin
Adams	Amash	Barletta
Aderholt	Amodei	Barr
Aguilar	Ashford	Barton

Bass
Beatty
Becerra
Benishek
Bera
Beyer
Bilirakis
Bishop (GA)
Bishop (MI)
Bishop (UT)
Black
Blackburn
Blum
Blumenauer
Bonamici
Bost
Brady (PA)
Brat
Bridenstine
Brooks (AL)
Brooks (IN)
Brown (FL)
Brownley (CA)
Buchanan
Buck
Bucshon
Burgess
Bustos
Byrne
Calvert
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
Coffman
Cohen
Cole
Collins (GA)
Collins (NY)
Comstock
Conaway
Connolly
Conyers
Cook
Cooper
Costa
Costello (PA)
Courtney
Cramer
Crawford
Crenshaw
Crowley
Cuellar
Culberson
Cummings
Curbelo (FL)
Davis (CA)
Davis, Danny
DeFazio
DeGette
Delaney
DeLauro
DelBene
Denham
Dent
DeSantis
DeSaulnier
DesJarlais
Deutch
Diaz-Balart
Dingell
Doggett
Dold
Doyle, Michael F.
Duckworth
Duffy
Duncan (SC)
Duncan (TN)
Edwards
Ellison
Ellmers (NC)
Emmer (MN)
Engel
Esty
Farenthold
Farr
Fattah
Fincher
Fitzpatrick
Fleischmann
Fleming
Flores
Forbes
Fortenberry
Foster
Foxx
Frankel (FL)
Franks (AZ)
Frelinghuysen
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
Guthrie
Gutiérrez
Hahn
Hanna
Hardy
Harper
Harris
Hartzler
Heck (NV)
Heck (WA)
Hensarling
Herrera Beutler
Hice, Jody B.
Higgins
Hill
Himes
Hinojosa
Holding
Honda
Hoyer
Hudson
Huelskamp
Huffman
Huizenga (MI)
Hultgren
Hunter
Hurd (TX)
Hurt (VA)
Israel
Issa
Jackson Lee
Jeffries
Jenkins (KS)
Jenkins (WV)
Johnson (GA)
Johnson (OH)
Johnson, Sam
Jolly
Jones
Jordan
Joyce
Katko
Keating
Kelly (IL)
Kelly (PA)
Kennedy
Kildee
Kilmer
Kind
King (IA)
King (NY)
Kinzinger (IL)
Kirkpatrick
Kline
Knight
Kuster
Labrador
Lamborn
Lance
Langevin
Larsen (WA)
Larson (CT)
Latta
Lawrence
Lee
Levin
Lewis
Lieu, Ted
LoBiondo
Loebsack
Lofgren
Long
Loudermilk
Love
Lowenthal
Lowey
Lucas
Luetkemeyer
Lujan Grisham (NM)
Luján, Ben Ray (NM)
Lummis
Lynch
MacArthur
Maloney, Carolyn
Maloney, Sean
Marino
Massie
Matsui
McCarthy
McCaul
McClintock
McCollum
McDermott
McGovern
McHenry
McKinley
McMorris Rodgers
McNerney
McSally
Meadows
Meehan
Meng
Messer
Mica
Miller (FL)
Miller (MI)
Moolenaar
Mooney (WV)
Moulton
Mullin
Mulvaney
Murphy (FL)
Murphy (PA)
Nadler
Napolitano
Neal
Neugebauer
Newhouse
Noem
Nolan
Norcross
Nugent
Nunes
O'Rourke
Palazzo
Palmer
Pascrell
Paulsen
Pearce
Pelosi
Perlmutter
Perry
Peters
Peterson
Pingree
Pittenger
Pitts
Pocan
Poe (TX)
Poliquin
Polis
Pompeo
Posey
Price (NC)
Price, Tom
Quigley
Rangel
Ratcliffe
Reed
Reichert
Renacci
Ribble
Rice (NY)
Rice (SC)
Richmond
Rigell
Roby
Roe (TN)
Rogers (AL)
Rogers (KY)
Rohrabacher
Rokita
Rooney (FL)
Ros-Lehtinen
Roskam
Ross
Rothfus
Rouzer
Roybal-Allard
Royce
Ruiz
Ruppersberger
Rush
Russell
Ryan (OH)
Ryan (WI)
Salmon
Sánchez, Linda T.
Sanchez, Loretta
Sanford
Sarbanes
Scalise
Schakowsky
Schiff
Schrader
Schweikert
Scott (VA)
Scott, Austin
Scott, David
Sensenbrenner
Serrano
Sessions
Sewell (AL)
Sherman
Shimkus
Shuster
Simpson
Sinema
Sires
Slaughter
Smith (MO)
Smith (NE)
Smith (NJ)
Smith (TX)
Stefanik
Stewart
Stivers
Stutzman
Swalwell (CA)
Takai
Takano
Thompson (CA)
Thompson (MS)
Thompson (PA)
Thornberry
Tiberi
Tipton
Titus
Tonko
Torres
Tsongas
Turner
Upton
Valadao
Van Hollen
Vargas
Veasey
Vela
Velázquez
Visclosky
Wagner
Walberg
Walden
Walker
Walorski
Walters, Mimi
Walz
Wasserman Schultz
Waters, Maxine
Watson Coleman
Webster (FL)
Welch
Wenstrup
Westerman
Whitfield
Williams
Wilson (FL)
Wilson (SC)
Wittman
Womack
Woodall
Yarmuth
Yoder
Yoho
Young (IA)
Young (IN)
Zeldin
Zinke

NOES—8

Boustany
Brady (TX)
Carter (TX)
LaMalfa
Marchant
Weber (TX)
Westmoreland
Young (AK)

NOT VOTING—18

Boyle, Brendan F.
Butterfield
Clyburn
Davis, Rodney
Eshoo
Graves (MO)
Hastings
Johnson, E. B.
Kaptur
Lipinski
Meeks
Moore
Olson
Pallone
Payne
Smith (WA)
Speier
Trott

□ 1130

Messrs. BUCSHON, POSEY, Mrs. MCMORRIS RODGERS, Messrs. BRIDENSTINE, COFFMAN, TIPTON, CRAWFORD, GIBBS, MILLER of Florida, and GOHMERT 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. HARPER). The question is on the amendment in the nature of a substitute.

The amendment was agreed to.

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

Accordingly, the Committee rose; and the Speaker pro tempore (Mr. FORTENBERRY) having assumed the chair, Mr. HARPER, 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. 1731) to amend the Homeland Security Act of 2002 to enhance multi-directional sharing of information related to cybersecurity risks and strengthen privacy and civil liberties protections, 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 amendment in the nature of a substitute, as amended.

The amendment was agreed to.

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

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

MOTION TO RECOMMIT

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

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

Mr. ISRAEL. I am, in its current form, Mr. Speaker.

Mr. MCCAUL. Mr. Chair, I reserve a point of order.

The SPEAKER pro tempore. A point of order is reserved.

The Clerk will report the motion to recommit.

The Clerk read as follows:

Mr. Israel moves to recommit the bill H.R. 1731 to the Committee on Homeland Security with instructions to report the same back to the House forthwith, with the following amendment:

Add at the end of the bill the following:

SEC. ___. PROTECTING CRITICAL INFRASTRUCTURE, AMERICAN JOBS, AND HEALTH INFORMATION FROM CYBERATTACKS.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended by adding at the end the following new section:

''SEC. 232. PROTECTING CRITICAL INFRASTRUCTURE, AMERICAN JOBS, AND HEALTH INFORMATION FROM CYBERATTACKS.

''(a) IN GENERAL.—The Secretary of Homeland Security shall undertake on-going risk-informed outreach, including the provision of technical assistance, to the owners and operators of at-risk critical infrastructure to promote the sharing of cyber threat indicators and defensive measures (as such terms are defined in the second section 226 (relating to the National Cybersecurity and Communications Integration Center). In carrying out this outreach, the Secretary shall prioritize the protection of at-risk Supervisory Control and Data Acquisition (SCADA) industrial control systems, which are critical to the operation of the United States economy.

''(b) PRIORITIZATION.—In carrying out outreach under subsection (a), the Secretary of Homeland Security shall prioritize the protection and welfare of the American people and economy and give special attention to protecting the following:

''(1) United States critical infrastructure, including the electrical grid, nuclear power plants, oil and gas pipelines, financial services, and transportation systems, from cyberattacks, as attacks on SCADA industrial control systems increased by 100 percent in 2014 over the previous year.

''(2) The intellectual property of United States corporations, particularly the intellectual property of at-risk small and medium-sized businesses, in order to maintain United States competitiveness and job growth.

''(3) The privacy and property rights of at-risk Americans, including Social Security numbers, dates of birth, and employment information, and health records, insofar as the health records of more than 29,000,000 Americans were compromised in data breaches between 2010 and 2013, and, in 2015, the information of 80,000,000 Americans was compromised by the attack on Anthem Health Insurance.''.

(b) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 231 the following new item:

''Sec. 232. Protecting critical infrastructure, American jobs, and health information from cyberattacks.''.

Mr. MCCAUL (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 Texas?

There was no objection.

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

Mr. ISRAEL. Mr. Speaker, this is a final amendment. It will not kill the bill. It will not send the bill back to committee. If adopted, the bill will immediately proceed to final passage, as amended.

Mr. Speaker, 2 weeks ago, D.C. went dark. The lights went out, the power stopped near the White House, lights out, no power at the Department of State. Federal agencies were plunged into darkness, small businesses plunged into darkness. Business stopped. The business of government stopped because there was a blackout.

Now, in this case, Mr. Speaker, this loss of energy was because of a blown transformer, and there was no indication that this was a result of a cyber attack on our energy sources or systems.

There are indications, Mr. Speaker, every day, of attempted attacks on our critical energy infrastructure, and this amendment simply strengthens the response of the Department of Homeland Security to protect our constituents, our government, our infrastructure, and our country from this attack.

Mr. Speaker, in the first 6 months of 2012, we know that there was a sustained and persistent cyber attack on critical gas pipeline control systems. Now, the good news is that we successfully defended against those attacks.

The bad news is, as we all know, the very nature of cyber war means that every time you defend against an attack, you are transmitting to your attackers what your defenses are.

The DHS reports that, of roughly 200 cases of major cyber attacks handled by DHS' cybersecurity team in 2013, 40 percent were in the energy sector. There have been attacks on supervisory control and data acquisitions, SCADA. Those attacks doubled between 2013 and 2014, so we know these attacks are being attempted. We know how serious it is.

We learned, 2 weeks ago, what happens when we plunge into the darkness. We know the economic devastation, the social devastation, the military devastation that will occur when an attack is successful, when a cyber attack against our energy systems succeeds.

We know it is coming, and we cannot wait until the day after, when we ask ourselves, in the dark: Why didn't we do more yesterday?

This is like being told that Pearl Harbor is coming, that 9/11 is coming, knowing it is coming, and deciding: Are you going to do something about it? Or are you going to continue to bury your head in the sand?

Now, this amendment is very simple, Mr. Speaker. It simply directs the Department of Homeland Security to organize a strong, concerted, focused partnership with energy companies throughout this country. Those partnerships would provide technical assistance from DHS to energy companies and information sharing. These partnerships would be focused on critical infrastructure, the electrical grid, oil and gas pipelines, and nuclear power plants.

Mr. Speaker, what happened in Washington, D.C., on April 7 of this year can happen in any congressional district in this body. Instead of a blown transformer, it will be a cyber attack against energy systems in any one of the districts represented here today, Mr. Speaker.

When that happens, our constituents will ask us, from that place in the dark: What did you do to prevent it? And what did you do to protect me from it?

This vote on this motion to recommit will be your answer.

Let's put the protection of our businesses, our government, our military, and our constituents ahead of partisanship and vote ''yes'' on this motion to recommit.

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

Mr. MCCAUL. Mr. Speaker, I withdraw my reservation of a point of order.

The SPEAKER pro tempore. The reservation of the point of order is withdrawn.

Mr. MCCAUL. Mr. Speaker, I rise today in strong opposition to the motion to recommit.

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

Mr. MCCAUL. The gentleman from New York is correct regarding the nature of the threat. However, the activities he has discussed were authorized by Congress last Congress with a bill that I sponsored. In addition, the bill currently before the House strengthens those provisions.

This bipartisan bill passed out of committee unanimously. This motion is nothing more than an eleventh hour attempt to bring down the bill that we worked so hard on to get to this point where we are today.

Mr. Speaker, people always ask me what keeps me up at night. In addition to the kinetic threats posed by al Qaeda and ISIS, it is a cyber attack against our Nation that concerns me the most.

This legislation is necessary to protect Americans. Every day, America is under attack. Our offensive capabilities are strong, but our defensive capabilities are weak. The attacks on Target and Home Depot stole the personal information and credit cards of millions of Americans.

The cyber breach at Anthem compromised the healthcare accounts of 80 million individuals, impacting one out of every four Americans in the most private way. North Korea's destructive attack on Sony attempted to chill our freedom of speech. Russia and China continue to steal our intellectual property and conduct espionage against our Nation.

General Alexander described this as ''the greatest transfer of wealth in history.''

At the same time, Iran attacks our financial sector on a daily basis in response to the sanctions. We also face a growing threat from cyberterrorists, like the ISIS sympathizers who hacked into USCENTCOM's social media account.

Terrorists and state sponsors of terror, like Iran, want nothing more than to carry out a destructive cyber attack to bring things down in the United States, including our power grids.

This bill protects our Nation's networks, both public and private, by removing legal barriers to the sharing of threat information.

□ 1145

The bill is voluntary. It is both proprivacy and prosecurity and has widespread support from industry. It allows us to obtain the keys for information sharing, to lock the door, and to keep these nation-states and criminals out. We cannot send a signal of weakness to our adversaries.

Many, Mr. Speaker, refer to the threat of a cyber Pearl Harbor. My father, part of the Greatest Generation, was a bombardier in a B–17 during World War II. He participated in the air campaign in advance of the D-day invasion against the Nazis.

Today a new generation faces different threats to our national security, and we must protect America in this new frontier. We now live in a new threat environment where digital bombs can go undetected and cause massive devastation. This bill will defend America from these attacks.

Inaction today, Mr. Speaker, would be nothing short of reckless. It is urgent that we pass this bill today, for if Congress fails to act and the United States is attacked, then Congress will have that on its hands.

I urge my colleagues to vote against the motion to recommit and support this bill.

I yield back the balance of my time.

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

There was no objection.

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

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

RECORDED VOTE

Mr. ISRAEL. 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 180, noes 238, not voting 13, as follows:

[Roll No. 172]

AYES—180

Adams
Aguilar
Ashford
Bass
Beatty
Becerra
Bera
Beyer
Bishop (GA)
Blumenauer
Bonamici
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
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.
Jones
Keating
Kelly (IL)
Kennedy
Kildee
Kilmer
Kind
Kirkpatrick
Kuster
Langevin
Larsen (WA)
Larson (CT)
Lawrence
Lee
Levin
Lewis
Lieu, Ted
Loebsack
Lofgren
Lowenthal
Lowey
Lujan Grisham (NM)
Luján, Ben Ray (NM)
Lynch
Maloney, Carolyn
Maloney, Sean
Matsui
McCollum
McDermott
McGovern
McNerney
Meeks
Meng
Moulton
Murphy (FL)
Nadler
Napolitano
Neal
Nolan
Norcross
O'Rourke
Pascrell
Payne
Pelosi
Perlmutter
Peters
Peterson
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
Swalwell (CA)
Takai
Takano
Thompson (CA)
Thompson (MS)
Titus
Tonko
Torres
Tsongas
Van Hollen
Vargas
Veasey
Vela
Velázquez
Visclosky
Walz
Wasserman Schultz
Waters, Maxine
Watson Coleman
Welch
Wilson (FL)
Yarmuth

NOES—238

Abraham
Aderholt
Allen
Amash
Amodei
Babin
Barletta
Barr
Barton
Benishek
Bilirakis
Bishop (MI)
Bishop (UT)
Black
Blackburn
Blum
Bost
Boustany
Brady (TX)
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
Curbelo (FL)
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
Jordan
Joyce
Katko
Kelly (PA)
King (IA)
King (NY)
Kinzinger (IL)
Kline
Knight
Labrador
LaMalfa
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
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
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—13

Boyle, Brendan F.
Davis, Rodney
Eshoo
Graves (MO)
Hastings
Kaptur
Lipinski
Moore
Olson
Pallone
Smith (WA)
Speier
Trott

□ 1153

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

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. McCAUL. 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 355, noes 63, not voting 13, as follows:

[Roll No. 173]

AYES—355

Abraham
Adams
Aderholt
Aguilar
Allen
Amodei
Ashford
Babin
Barletta
Barr
Barton
Beatty
Benishek
Bera
Beyer
Bilirakis
Bishop (GA)
Bishop (MI)
Bishop (UT)
Black
Blackburn
Blum
Bonamici
Bost
Boustany
Brady (TX)
Brooks (AL)
Brooks (IN)
Brown (FL)
Brownley (CA)
Buchanan
Buck
Bucshon
Burgess
Bustos
Butterfield
Byrne
Calvert
Capps
Cárdenas
Carney
Carson (IN)
Carter (GA)
Carter (TX)
Castor (FL)
Castro (TX)
Chabot
Chaffetz
Clarke (NY)
Clawson (FL)
Clay
Cleaver
Clyburn
Coffman
Cohen
Cole
Collins (GA)
Collins (NY)
Comstock
Conaway
Connolly
Cook
Cooper
Costa
Costello (PA)
Cramer
Crawford
Crenshaw
Crowley
Cuellar
Culberson
Cummings
Curbelo (FL)
Davis (CA)
Davis, Danny
DeFazio
DeGette
Delaney
DelBene
Denham
Dent
DeSantis
DeSaulnier
Diaz-Balart
Dingell
Doggett
Dold
Duckworth
Duffy
Duncan (SC)
Duncan (TN)
Ellmers (NC)
Emmer (MN)
Engel
Farenthold
Farr
Fincher
Fitzpatrick
Fleischmann
Flores
Forbes
Fortenberry
Foster
Foxx
Frankel (FL)
Franks (AZ)
Frelinghuysen
Fudge
Gabbard
Gallego
Garamendi
Gibbs
Gibson
Goodlatte
Gowdy
Graham
Granger
Graves (GA)
Green, Al
Green, Gene
Griffith
Grothman
Guthrie
Gutiérrez
Hahn
Hanna
Hardy
Harper
Harris
Hartzler
Heck (NV)
Heck (WA)
Hensarling
Herrera Beutler
Hice, Jody B.
Higgins
Hill
Himes
Hinojosa
Holding
Honda
Hoyer
Hudson
Huffman
Huizenga (MI)
Hultgren
Hunter
Hurd (TX)
Hurt (VA)
Israel
Jackson Lee
Jeffries
Jenkins (KS)
Jenkins (WV)
Johnson (GA)
Johnson (OH)
Johnson, Sam
Jolly
Joyce
Katko
Keating
Kelly (IL)
Kelly (PA)
Kennedy
Kildee
Kilmer
Kind
King (IA)
King (NY)
Kinzinger (IL)
Kirkpatrick
Kline
Knight
Kuster
LaMalfa
Lamborn
Lance
Langevin
Larsen (WA)
Latta
Lawrence
Levin
Lewis
LoBiondo
Loebsack
Lofgren
Long
Loudermilk
Love
Lowey
Lucas
Luetkemeyer
Lujan Grisham (NM)
Luján, Ben Ray (NM)
Lummis
Lynch
MacArthur
Maloney, Carolyn
Maloney, Sean
Marchant
Marino
Matsui
McCarthy
McCaul
McClintock
McCollum
McDermott
McHenry
McKinley
McMorris Rodgers
McNerney
McSally
Meadows
Meehan
Meeks
Meng
Messer
Mica
Miller (FL)
Miller (MI)
Moolenaar
Moulton
Mullin
Mulvaney
Murphy (FL)
Murphy (PA)
Napolitano
Neal
Neugebauer
Newhouse
Noem
Norcross
Nugent
Nunes
O'Rourke
Palazzo
Palmer
Pascrell
Paulsen
Payne
Pearce
Pelosi
Perlmutter
Perry
Peters
Peterson
Pittenger
Pitts
Poe (TX)
Poliquin
Pompeo
Posey
Price (NC)
Price, Tom
Quigley
Rangel
Ratcliffe
Reed
Reichert
Renacci
Ribble
Rice (NY)
Rice (SC)
Richmond
Rigell
Roby
Roe (TN)
Rogers (AL)
Rogers (KY)
Rohrabacher
Rokita
Rooney (FL)
Ros-Lehtinen
Roskam
Ross
Rothfus
Rouzer
Roybal-Allard
Royce
Ruiz
Ruppersberger
Rush
Russell
Ryan (WI)

Sánchez, Linda T.	Stefanik	Walker
Sanchez, Loretta	Stewart	Walorski
Scalise	Stivers	Walters, Mimi
Schakowsky	Stutzman	Walz
Schiff	Swalwell (CA)	Watson Coleman
Schrader	Takai	Weber (TX)
Schweikert	Thompson (CA)	Webster (FL)
Scott (VA)	Thompson (MS)	Wenstrup
Scott, Austin	Thompson (PA)	Westerman
Scott, David	Thornberry	Westmoreland
Sensenbrenner	Tiberi	Whitfield
Sessions	Tipton	Williams
Sewell (AL)	Titus	Wilson (FL)
Sherman	Torres	Wilson (SC)
Shimkus	Turner	Wittman
Shuster	Upton	Womack
Simpson	Valadao	Woodall
Sinema	Vargas	Yoder
Sires	Veasey	Yoho
Smith (MO)	Vela	Young (AK)
Smith (NE)	Visclosky	Young (IA)
Smith (NJ)	Wagner	Young (IN)
Smith (TX)	Walberg	Zeldin
	Walden	Zinke

NOES—63

Amash	Fattah	Nadler
Bass	Fleming	Nolan
Becerra	Garrett	Pingree
Blumenauer	Gohmert	Pocan
Brady (PA)	Gosar	Polis
Brat	Graves (LA)	Ryan (OH)
Bridenstine	Grayson	Salmon
Capuano	Grijalva	Sanford
Cartwright	Guinta	Sarbanes
Chu, Judy	Huelskamp	Serrano
Cicilline	Issa	Slaughter
Clark (MA)	Johnson, E. B.	Takano
Conyers	Jones	Tonko
Courtney	Jordan	Tsongas
DeLauro	Labrador	Van Hollen
DesJarlais	Larson (CT)	Velázquez
Deutch	Lee	Wasserman Schultz
Doyle, Michael F.	Lieu, Ted	Waters, Maxine
Edwards	Lowenthal	Welch
Ellison	Massie	Yarmuth
Esty	McGovern	
	Mooney (WV)	

NOT VOTING—13

Boyle, Brendan F.	Hastings	Pallone
Davis, Rodney	Kaptur	Smith (WA)
Eshoo	Lipinski	Speier
Graves (MO)	Moore	Trott
	Olson	

□ 1203

So the bill was passed.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

The SPEAKER pro tempore. Pursuant to section 3 of House Resolution 212, the text of H.R. 1731 was appended to the engrossment of H.R. 1560, and H.R. 1731 was laid on the table.

PERMISSION FOR MEMBER TO BE CONSIDERED AS FIRST SPONSOR OF H.R. 637

Mr. PAULSEN. Mr. Speaker, I ask unanimous consent that I may hereafter be considered as the first sponsor of H.R. 637, a bill originally introduced by Representative Schock of Illinois, for the purposes of adding cosponsors and requesting reprintings pursuant to clause 7 of rule XII.

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

There was no objection.

MOMENT OF SILENCE TO PAY RESPECTS TO THE YOUNG WOMEN WHO DIED SUDDENLY IN SAVANNAH, GEORGIA, APRIL 22, 2015

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

Mr. CARTER of Georgia. Mr. Speaker, I rise today to pay my respects to the young women who died suddenly in Savannah, Georgia, yesterday. On Wednesday morning just before 6 a.m., three tractor-trailers, two pickup trucks, and two cars were involved in a chain-reaction car accident.

Abbie Deloach of Savannah, Emily Clark of Powder Springs, Morgan Bass of Leesburg, Catherine McKay Pittman of Alpharetta, and Caitlyn Baggett of Millen were killed.

I ask that a moment of silence be given to these young women and their families in the Eagle Nation.

LEGISLATIVE PROGRAM

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

Mr. HOYER. Mr. Speaker, I yield to the majority leader, Mr. MCCARTHY, for the purpose of inquiring about the schedule of the week to come.

Mr. MCCARTHY. I thank the gentleman for yielding.

Mr. Speaker, on Monday, no votes are expected in the House. On Tuesday, the House will meet at noon for morning hour and 2 p.m. for legislative business. Votes will be postponed until 6:30. On Wednesday and Thursday, the House will meet at 10 a.m. for morning hour and noon for legislative business. On Friday, the House will meet at 9 a.m. for legislative business. Last votes of the week are expected no later than 3 p.m.

Mr. Speaker, the House will consider a number of suspensions next week, a complete list of which will be announced by close of business tomorrow.

In addition, the House will begin the annual appropriation process. The House will consider the Military Construction and Veterans Affairs appropriations bill sponsored by Representative CHARLIE DENT. This important bill provides funding to house and train our military and ensures that we can meet the growing health care needs of our Nation's veterans.

The House will also consider the Energy and Water appropriations bill sponsored by Representative MIKE SIMPSON. This bill ensures that we safely maintain our nuclear weapons stockpile and provide for critical infrastructure projects through the Army Corps of Engineers.

Finally, Mr. Speaker, the House is expected to consider the budget conference report. I thank the gentleman.

Mr. HOYER. I thank the gentleman for that information. He indicates that the appropriations process has started. First I want to say, as a Member who served on the Appropriations Committee for 23 years, I always thought we ought to start the appropriations process early, i.e., in May, but starting it, I think, is good news. We have had trouble on both sides getting all 12 appropriations bills—it used to be 13—12 appropriations bills done. So I congratulate the committee for initiating its work in a timely fashion.

Hopefully, Mr. Leader, that will lead to, hopefully, passing 12 bills in the regular order, which, as I pointed out last week with respect to some other legislation, will require the kind of bipartisanship that we saw displayed ultimately on the DHS bill, but certainly on the SGR bill, and then this week we had two bills pass with a bipartisan—both sides—majority voting for it. Hopefully, we will be able to do that on the appropriations bill.

I ask my friend on the MILCON, Military Construction bill, VA funding bill and on the Energy and Water bill, does the gentleman expect to follow what the gentleman and his party have indicated would be the process for appropriation bills under an open rule?

I yield to my friend.

Mr. MCCARTHY. I thank the gentleman for yielding.

The answer to your question is ''yes.'' The gentleman does know, having been a part for many years of the appropriation process, that this is actually the earliest in the history of Congress we have ever started appropriations. It is our goal—I know it is your goal as well—to get all bills done through the House in regular order. It is something that we strive towards, and I thank the gentleman for his help.

Mr. HOYER. I congratulate the gentleman and his party on bringing these bills to the floor early.

He also says we are going to be considering a conference report. I don't obviously know what that conference report is. The budget itself, though—which of course sets the parameters for the appropriations bills in terms of caps on spending—was, as the gentleman knows, not a bipartisan bill. There were party differences on that bill. I would hope that in the conference report we can reach an agreement.

My own view is, Mr. Majority Leader, that if we stay at sequester levels we will not be able to pass bills and the President will not sign them. The reason being that our side, and I think the President, perceives, and many in your party perceive at least as it relates to some aspects of the sequester, that the sequester numbers are not workable.

As you know, the chairman of the Appropriations Committee has called the sequester numbers, which are reflected in the budget that passed the House, ill-conceived, unworkable, and unrealistic. In that context it will be difficult for us to get, no matter how early we start, these bills completed. I would hope that we could come together at some point in time as was done in Ryan-Murray. I know there are Members on your side, including I think the chairman of the Appropriations Committee, who believe that if we don't come together on an agreed figure that will allow the Appropriations Committee to meet its responsibilities, then we will have great difficulty getting appropriations bills done.

I don't know whether the gentleman has any thoughts on that, but if he does, I would be glad to yield to him on that.