generation of cyber-prepared warriors for our country is at the heart of what the gentlewoman is trying to do, to enable universities and others to develop these kinds of programs that support students who, in return for some support for their education, will come to work for us. That will get us the next level of individuals, and it will begin the process of training those individuals, which we will need.

So this is, again, another important piece of our overall successful approach to trying to create cybersecurity.

I urge all of the Members to join me in supporting this bill, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Pennsylvania (Mr. MEEHAN) that the House suspend the rules and concur in the Senate amendment to the bill, H.R. 2952.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the Senate amendment was concurred in.

A motion to reconsider was laid on the table.

NATIONAL CYBERSECURITY PROTECTION ACT OF 2014

Mr. MCCAUL. Mr. Speaker, I move to suspend the rules and pass the bill (S. 2519) to codify an existing operations center for cybersecurity.

The Clerk read the title of the bill.

The text of the bill is as follows:

S. 2519

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 Act of 2014''.

SEC. 2. DEFINITIONS.

In this Act—

(1) the term ''Center'' means the national cybersecurity and communications integration center under section 226 of the Homeland Security Act of 2002, as added by section 3;

(2) the term ''critical infrastructure'' has the meaning given that term in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101);

(3) the term ''cybersecurity risk'' has the meaning given that term in section 226 of the Homeland Security Act of 2002, as added by section 3;

(4) the term ''information sharing and analysis organization'' has the meaning given that term in section 212(5) of the Homeland Security Act of 2002 (6 U.S.C. 131(5));

(5) the term ''information system'' has the meaning given that term in section 3502(8) of title 44, United States Code; and

(6) the term ''Secretary'' means the Secretary of Homeland Security.

SEC. 3. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(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:

''SEC. 226. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

''(a) DEFINITIONS.—In this section—

''(1) 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 information or information systems, including such related consequences caused by an act of terrorism;

''(2) the term 'incident' means an occurrence that—

''(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system; or

''(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies;

''(3) the term 'information sharing and analysis organization' has the meaning given that term in section 212(5); and

''(4) the term 'information system' has the meaning given that term in section 3502(8) of title 44, United States Code.

''(b) CENTER.—There is in the Department a national cybersecurity and communications integration center (referred to in this section as the 'Center') to carry out certain responsibilities of the Under Secretary appointed under section 103(a)(1)(H).

''(c) FUNCTIONS.—The cybersecurity functions of the Center shall include—

''(1) being a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities;

''(2) providing shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government and non-Federal entities to address cybersecurity risks and incidents to Federal and non-Federal entities;

''(3) coordinating the sharing of information related to cybersecurity risks and incidents across the Federal Government;

''(4) facilitating cross-sector coordination to address cybersecurity risks and incidents, including cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors;

''(5)(A) conducting integration and analysis, including cross-sector integration and analysis, of cybersecurity risks and incidents; and

''(B) sharing the analysis conducted under subparagraph (A) with Federal and non-Federal entities;

''(6) upon request, providing timely technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to cybersecurity risks and incidents, which may include attribution, mitigation, and remediation; and

''(7) providing information and recommendations on security and resilience measures to Federal and non-Federal entities, including information and recommendations to—

''(A) facilitate information security; and

''(B) strengthen information systems against cybersecurity risks and incidents.

''(d) COMPOSITION.—

''(1) IN GENERAL.—The Center shall be composed of—

''(A) appropriate representatives of Federal entities, such as—

''(i) sector-specific agencies;

''(ii) civilian and law enforcement agencies; and

''(iii) elements of the intelligence community, as that term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4));

''(B) appropriate representatives of non-Federal entities, such as—

''(i) State and local governments;

''(ii) information sharing and analysis organizations; and

''(iii) owners and operators of critical information systems;

''(C) components within the Center that carry out cybersecurity and communications activities;

''(D) a designated Federal official for operational coordination with and across each sector; and

''(E) other appropriate representatives or entities, as determined by the Secretary.

''(2) INCIDENTS.—In the event of an incident, during exigent circumstances the Secretary may grant a Federal or non-Federal entity immediate temporary access to the Center.

''(e) PRINCIPLES.—In carrying out the functions under subsection (c), the Center shall ensure—

''(1) to the extent practicable, that—

''(A) timely, actionable, and relevant information related to cybersecurity risks, incidents, and analysis is shared;

''(B) when appropriate, information related to cybersecurity risks, incidents, and analysis is integrated with other relevant information and tailored to the specific characteristics of a sector;

''(C) activities are prioritized and conducted based on the level of risk;

''(D) industry sector-specific, academic, and national laboratory expertise is sought and receives appropriate consideration;

''(E) continuous, collaborative, and inclusive coordination occurs—

''(i) across sectors; and

''(ii) with—

''(I) sector coordinating councils;

''(II) information sharing and analysis organizations; and

''(III) other appropriate non-Federal partners;

''(F) as appropriate, the Center works to develop and use mechanisms for sharing information related to cybersecurity risks and incidents that are technology-neutral, interoperable, real-time, cost-effective, and resilient; and

''(G) the Center works with other agencies to reduce unnecessarily duplicative sharing of information related to cybersecurity risks and incidents;

''(2) that information related to cybersecurity risks and incidents is appropriately safeguarded against unauthorized access; and

''(3) that activities conducted by the Center comply with all policies, regulations, and laws that protect the privacy and civil liberties of United States persons.

''(f) NO RIGHT OR BENEFIT.—

''(1) IN GENERAL.—The provision of assistance or information to, and inclusion in the Center of, governmental or private entities under this section shall be at the sole and unreviewable discretion of the Under Secretary appointed under section 103(a)(1)(H).

''(2) CERTAIN ASSISTANCE OR INFORMATION.—The provision of certain assistance or information to, or inclusion in the Center of, one governmental or private entity pursuant to this section shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 note) is amended by inserting after the item relating to section 225 the following:

''Sec. 226. National cybersecurity and communications integration center.''.

SEC. 4. RECOMMENDATIONS REGARDING NEW AGREEMENTS.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary shall submit recommendations on how to expedite the implementation of information-sharing agreements for cybersecurity purposes between the Center and non-Federal entities (referred to in this section as ''cybersecurity information-sharing agreements'') to—

(1) the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate; and

(2) the Committee on Homeland Security and the Committee on the Judiciary of the House of Representatives.

(b) CONTENTS.—In submitting recommendations under subsection (a), the Secretary shall—

(1) address the development and utilization of a scalable form that retains all privacy and other protections in cybersecurity information-sharing agreements that are in effect as of the date on which the Secretary submits the recommendations, including Cooperative Research and Development Agreements; and

(2) include in the recommendations any additional authorities or resources that may be needed to carry out the implementation of any new cybersecurity information-sharing agreements.

SEC. 5. ANNUAL REPORT.

Not later than 1 year after the date of enactment of this Act, and every year thereafter for 3 years, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate, the Committee on Homeland Security and the Committee on the Judiciary of the House of Representatives, and the Comptroller General of the United States a report on the Center, which shall include—

(a) information on the Center, including—

(1) an assessment of the capability and capacity of the Center to carry out its cybersecurity mission under this Act;

(2) the number of representatives from non-Federal entities that are participating in the Center, including the number of representatives from States, nonprofit organizations, and private sector entities, respectively;

(3) the number of requests from non-Federal entities to participate in the Center and the response to such requests;

(4) the average length of time taken to resolve requests described in paragraph (3);

(5) the identification of—

(A) any delay in resolving requests described in paragraph (3) involving security clearance processing; and

(B) the agency involved with a delay described in subparagraph (A);

(6) a description of any other obstacles or challenges to resolving requests described in paragraph (3) and a summary of the reasons for denials of any such requests;

(7) the extent to which the Department is engaged in information sharing with each critical infrastructure sector, including—

(A) the extent to which each sector has representatives at the Center;

(B) the extent to which owners and operators of critical infrastructure in each critical infrastructure sector participate in information sharing at the Center; and

(C) the volume and range of activities with respect to which the Secretary has collaborated with the sector coordinating councils and the sector-specific agencies to promote greater engagement with the Center; and

(8) the policies and procedures established by the Center to safeguard privacy and civil liberties.

SEC. 6. GAO REPORT.

Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the effectiveness of the Center in carrying out its cybersecurity mission.

SEC. 7. CYBER INCIDENT RESPONSE PLAN; CLEARANCES; BREACHES.

(a) CYBER INCIDENT RESPONSE PLAN; CLEARANCES.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.), as amended by section 3, is amended by adding at the end the following:

''SEC. 227. CYBER INCIDENT RESPONSE PLAN.

''The Under Secretary appointed under section 103(a)(1)(H) shall, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, information sharing and analysis organizations (as defined in section 212(5)), owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks (as defined in section 226) to critical infrastructure.

''SEC. 228. CLEARANCES.

''The Secretary shall make available the process of application for security clearances under Executive Order 13549 (75 Fed. Reg. 162; relating to a classified national security information program) or any successor Executive Order to appropriate representatives of sector coordinating councils, sector information sharing and analysis organizations (as defined in section 212(5)), owners and operators of critical infrastructure, and any other person that the Secretary determines appropriate.''.

(b) BREACHES.—

(1) REQUIREMENTS.—The Director of the Office of Management and Budget shall ensure that data breach notification policies and guidelines are updated periodically and require—

(A) except as provided in paragraph (4), notice by the affected agency to each committee of Congress described in section 3544(c)(1) of title 44, United States Code, the Committee on the Judiciary of the Senate, and the Committee on Homeland Security and the Committee on the Judiciary of the House of Representatives, which shall—

(i) be provided expeditiously and not later than 30 days after the date on which the agency discovered the unauthorized acquisition or access; and

(ii) include—

(I) information about the breach, including a summary of any information that the agency knows on the date on which notification is provided about how the breach occurred;

(II) an estimate of the number of individuals affected by the breach, based on information that the agency knows on the date on which notification is provided, including an assessment of the risk of harm to affected individuals;

(III) a description of any circumstances necessitating a delay in providing notice to affected individuals; and

(IV) an estimate of whether and when the agency will provide notice to affected individuals; and

(B) notice by the affected agency to affected individuals, pursuant to data breach notification policies and guidelines, which shall be provided as expeditiously as practicable and without unreasonable delay after the agency discovers the unauthorized acquisition or access.

(2) NATIONAL SECURITY; LAW ENFORCEMENT; REMEDIATION.—The Attorney General, the head of an element of the intelligence community (as such term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)), or the Secretary may delay the notice to affected individuals under paragraph (1)(B) if the notice would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions.

(3) OMB REPORT.—During the first 2 years beginning after the date of enactment of this Act, the Director of the Office of Management and Budget shall, on an annual basis—

(A) assess agency implementation of data breach notification policies and guidelines in aggregate; and

(B) include the assessment described in clause (i) in the report required under section 3543(a)(8) of title 44, United States Code.

(4) EXCEPTION.—Any element of the intelligence community (as such term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)) that is required to provide notice under paragraph (1)(A) shall only provide such notice to appropriate committees of Congress.

(c) RULE OF CONSTRUCTION.—Nothing in the amendment made by subsection (a) or in subsection (b)(1) shall be construed to alter any authority of a Federal agency or department.

(d) TECHNICAL AND CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 note), as amended by section 3, is amended by inserting after the item relating to section 226 the following:

''Sec. 227. Cyber incident response plan.
''Sec. 228. Clearances.''.

SEC. 8. RULES OF CONSTRUCTION.

(a) PROHIBITION ON NEW REGULATORY AUTHORITY.—Nothing in this Act or the amendments made by this Act shall be construed to grant the Secretary any authority to promulgate regulations or set standards relating to the cybersecurity of private sector critical infrastructure that was not in effect on the day before the date of enactment of this Act.

(b) PRIVATE ENTITIES.—Nothing in this Act or the amendments made by this Act shall be construed to require any private entity—

(1) to request assistance from the Secretary; or

(2) that requested such assistance from the Secretary to implement any measure or recommendation suggested by the Secretary.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Texas (Mr. MCCAUL) and the gentleman from Mississippi (Mr. THOMPSON) each will control 20 minutes.

The Chair recognizes the gentleman from Texas.

GENERAL LEAVE

Mr. MCCAUL. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days in which to revise and extend their remarks and to include any extraneous material on the bill under consideration.

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

There was no objection.

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

Mr. Speaker, I would like to, first, start out by thanking—this was not one person. This was a huge team effort, both in a bipartisan way and bicameral way. I want to thank PAT

MEEHAN for his great leadership on this. I want to thank YVETTE CLARKE for her great work and BENNIE THOMPSON for being willing to come together in a bipartisan way on our committee to get something good done for the American people.

I want to thank Senators CARPER and COBURN for moving forward—not something that we see much this Congress, something actually coming out of the Senate back to the House to pass out of this Congress, something we haven't seen much these days.

I also want to thank the staff. I want to thank Alex Manning, who is the staff director, and Brett DeWitt for his great work, tireless hours, and on the Democrat side of the House as well, holding over 300 meetings with the private sector, working day in and day out to get to the point where we are today on the House floor.

Mr. Speaker, I consider this to be a historic moment on the House floor, as we pass the most significant cybersecurity legislation ever passed by the Congress. This issue 10 years ago, no one would understand it. Today, people are finally starting to wake up to the fact that the threats from a cyber attack are real.

As we look at threats from China, from Russia, from Iran, we look at the theft of IP—a lot of people have been hurt personally with Home Depot and Target—we look at the theft of intellectual property from Russia and China, we look at the espionage on a daily basis, every Federal agency being hacked into, including the Pentagon, to steal things out of this Federal Government, to hurt our national security, and then, finally, we look at the most malicious threat, and that is a threat to shut things down.

We saw recently, Mr. Speaker, an attack from Iran that shut down 30,000 hard drives of Aramco, the largest energy producer in Saudi Arabia, while simultaneously hitting our financial sector. They continue to hit our financial sector every day. They are hitting them as I speak right now. We look at power grids being brought down and water and energy. This threat is real. This threat must be dealt with.

I am pleased on the very last day of this Congress that we are going to pass legislation that is going to protect America and make it safer, that is going to protect our critical infrastructures from this daily attack by foreign enemies that we have, unfortunately, across the globe.

□ 1015

How will that work? This bill will codify what is called the NCCIC. The National Cybersecurity Protection Act will create and codify a cyber command structure within DHS, the Department of Homeland Security, that is a civilian interface to the private sector which has been supported by both business groups like the Chamber and privacy groups like the ACLU.

It is amazing how we can bring this coalition together, but that is how strong this bill is: privacy and business coming together, doing what is right.

This will create a safe harbor, Mr. Speaker, where the 16 critical infrastructures, the 16 sectors, can come together. The Federal Government can take our threat information, our malicious codes that they use to attack us, and share that with the private sector. It also allows the private sector to share the information that they have with the Federal Government in a safe harbor that is protected both businesswise and personally as well.

Eighty to 85 percent of this threat information lies in the private sector. This coalition, if you will, this partnership of information sharing will better protect our critical infrastructures, and most importantly, to have the 16 sectors on the floor at the Department of Homeland Security, at the cyber command, and at the NCCIC all on the floor together sharing information, not just public and private, but amongst the sectors themselves—which is not taking place today—will go a long way to protecting American people and our critical infrastructures.

We have great offensive capability in this country. Our military has great cyber offensive capability to shut things down; in the wrong hands, that makes us very vulnerable. Where our weakness, our vulnerability lies is our ability to defend the Nation against these cyber attacks, and they are getting worse and more malicious by countries and state actors that don't really like us and want to do us harm.

I am proud of the work that we have done. I am proud of the work we have done in a bipartisan way, the work this committee has done, and I am proud of what the Senate has finally achieved to bring this finally to the point where we can pass this bill out of the United States Congress and have it signed into law by the President of the United States.

At the end of the day, it is what we got elected here to do, and that is to do good things to govern and get good things done on behalf of the American people.

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

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

Mr. Speaker, I rise in strong support of the Senate amendment to S. 2519, the National Cybersecurity Protection Act of 2014. This bipartisan measure is a product of extensive bicameral negotiations and, in many ways, the culmination of years of oversight work by this committee.

It not only sends a strong message of support for the Department of Homeland Security as the lead civilian agency for cybersecurity, but also pays special attention to the challenge of bolstering network security for critical infrastructure.

Over the past decade, Americans have come to understand the need for cybersecurity to be woven into everything that a company, government, or an individual does, from running the most intricate machinery to everyday participation in social media.

Americans used to depend on the two oceans to protect us from invasion. Interconnectedness resulting from advancement in technology has fostered great economic, scientific, social, and cultural rewards. At the same time, their interconnectedness allows our enemies to do harm without ever stepping foot on U.S. soil.

One of the strengths of S. 2519 is that it emphasizes voluntary information sharing and collaboration between the Department and critical infrastructure owners and operators to address this national threat. Importantly, it does so in a manner that is consistent with our constitutional values and principles.

Much like the House-passed version of this measure, H.R. 3696, that was heralded by the ACLU as ''pro-security and pro-privacy,'' the measure under consideration today effectively avoids the privacy and civil liberties pitfalls that have plagued other cyber information-sharing legislation.

S. 2519 leverages existing private-public partnerships such as information sharing and analysis centers and sector coordinating councils to foster better information sharing and does so without dangling the controversial liability protection ''carrot'' before companies. The opportunity to access timely threat information from a Federal civilian agency should be carrot enough to motivate companies to engage with DHS.

The legislation before us today represents an important moment for the committee and the 113th Congress. At the beginning of this Congress, expectations were high for some legislative action in the area of cybersecurity. It has taken some time to get here, but what we have before us is something solid that sets forth what DHS must do as a lead civilian agency for cybersecurity.

We have seen cybersecurity legislation fail to become law multiple times. While President Obama's executive order is making progress in attempts to shore up some cyber weaknesses in our Nation's fabric, more work needs to be done.

With this cybersecurity legislation, we will be doing our part as DHS authorizers to raise the level of cybersecurity, particularly within the Federal Government and protecting our Nation's critical infrastructure.

I reserve the balance of my time.

Mr. MCCAUL. Mr. Speaker, I yield such time as he may consume to the distinguished gentleman from Pennsylvania (Mr. MEEHAN).

Let me also, on a point of privilege, say what an honor it has been to serve with you, sir. We are going to miss you on this committee.

Mr. MEEHAN. Mr. Speaker, let me thank the gentleman again for his leadership not just on this particular issue, but his leadership of the committee and, as I had said before, working with my colleagues on the other

side in a bipartisan fashion for these important issues.

I will be brief on this, but I can tell you that it is not the brevity of my words that will instill the seriousness of this issue. When the chairman mentioned that this is some of the most important legislation we have ever done on cybersecurity, I echo that sentiment because the nature of the threat is real, growing, and constantly changing.

The ability for us to be able to be adaptive in real time to communicate with the private sector and the government facilities to protect our homeland is critical.

A second point—and that is significant as well—is very real attention was paid to the issue of privacy, recognizing the individual desire to be assured that private information is not inappropriately utilized or misapplied by anybody, let alone the government.

This bill was the product of work that was done in detail with over 300 different meetings working through the complexities of this particular issue. As has already been articulated, it is one of the few bills that I would imagine in this Congress—or any Congress—that has strong endorsement from the Chamber of Commerce and the ACLU simultaneously.

Lastly, by organizing by sector, this creates the framework. This is the important foundation. There is still so much more to be done, but this is the foundation of the house, of the structure that will allow us to create and continue to create the kind of edifice that will enable our private sector, our government sector, and indeed all of those who are engaged in this issue in the country to be better positioned to protect Americans, their information, and their safety.

I strongly endorse this, and I thank the gentleman for his leadership.

Mr. THOMPSON of Mississippi. Mr. Speaker, I yield such time as she may consume to the gentlewoman from New York (Ms. CLARKE), the ranking member of the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.

Ms. CLARKE of New York. Mr. Speaker, again, I thank the ranking member for yielding me the time.

Mr. Speaker, I rise in support of S. 2519, the National Cybersecurity Protection Act of 2014. We have worked long and hard to develop and describe how DHS can best accomplish its complex cybersecurity mission. I am pleased that our bipartisan and bicameral negotiations have been fruitful and look forward to the progress that the Department can make next year.

In closing, I would like to express what an honor it has been to serve under the leadership of Ranking Member THOMPSON, Chairman MCCAUL, and alongside Chairman MEEHAN in service to the homeland security mission of our Nation.

I look forward to our continued collaboration as I move to my new assignment on the Energy and Commerce Committee in the 114th Congress.

Mr. MCCAUL. Mr. Speaker, I have no further speakers, and I reserve the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Speaker, I rise in strong support of this legislation and thank my principal partner in the House, Chairman MCCAUL, for his unwavering commitment to this issue and willingness to work across the aisle to get it done.

I also want to recognize the contributions of the chairman and ranking member of the Cybersecurity Subcommittee, Representatives MEEHAN and CLARKE, and our Senate partners.

Finally, I would like to acknowledge staff that helped us get this to this point, Rosaline Cohen and Chris Schepis on my staff and Brett DeWitt and Alex Manning on the majority staff.

Again, let me compliment the chair for not giving up and for staying the course. Even doing it on the last day gets it done.

Mr. Speaker, I urge a ''yea'' vote, and I yield back the balance of my time.

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

I too want to recognize all the Members involved, the Senate, and staff. To my ranking member, BENNIE THOMPSON, I guess, as Churchill said:

Never, ever give up.

Here we are on the last day of this Congress getting this done. What a gratifying experience it is. What a great moment it is not just for this Congress but, more importantly, for the American people and what it represents.

Seventy-three years ago this week, this Nation was attacked at Pearl Harbor. There are a lot of people that make analogies to what would be a cyber Pearl Harbor if we are caught unprepared. I believe this bill will go a long way to defending the Nation from what would be called a cyber Pearl Harbor event.

My father served as a B–17 bombardier in the European theater. He flew over 32 missions, including the air campaign in advance of the D-day invasion and the Battle of the Bulge. They dropped kinetic bombs.

In the cyber world that we live in, we have to worry about digital bombs and how we can stop that from hurting the United States, from impacting the United States, from bringing the United States to its knees. I believe this is the first step of many, and I look forward to working on more legislation next Congress, but this is the historic first step that we have taken in this Congress to move forward on this very important issue and get it done to protect the American people.

With that, let me again thank everyone for their efforts. This has been a great day for America.

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

□ 1030

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Texas (Mr. MCCAUL) that the House suspend the rules and pass the bill, S. 2519.

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

A motion to reconsider was laid on the table.

PROVIDING FOR CONSIDERATION OF THE SENATE AMENDMENT TO H.R. 83, INSULAR AREAS AND FREELY ASSOCIATED STATES ENERGY DEVELOPMENT; WAIVING REQUIREMENT OF CLAUSE 6(A) OF RULE XIII WITH RESPECT TO CONSIDERATION OF CERTAIN RESOLUTIONS; AND FOR OTHER PURPOSES

Mr. COLE. Mr. Speaker, by direction of the Committee on Rules, I call up House Resolution 776 and ask for its immediate consideration.

The Clerk read the resolution, as follows:

H. RES. 776

Resolved, That upon adoption of this resolution it shall be in order to take from the Speaker's table the bill (H.R. 83) to require the Secretary of the Interior to assemble a team of technical, policy, and financial experts to address the energy needs of the insular areas of the United States and the Freely Associated States through the development of energy action plans aimed at promoting access to affordable, reliable energy, including increasing use of indigenous clean-energy resources, and for other purposes, with the Senate amendment thereto, and to consider in the House, without intervention of any point of order, a motion offered by the chair of the Committee on Appropriations or his designee that the House concur in the Senate amendment with an amendment consisting of the text of Rules Committee Print 113-59 modified by the amendment printed in the report of the Committee on Rules accompanying this resolution. The Senate amendment and the motion shall be considered as read. The motion shall be debatable for 80 minutes, with 60 minutes equally divided and controlled by the chair and ranking minority member of the Committee on Appropriations and 20 minutes equally divided and controlled by the chair and ranking minority member of the Committee on Education and the Workforce. The previous question shall be considered as ordered on the motion to its adoption without intervening motion.

SEC. 2. Upon adoption of the motion specified in the first section of this resolution, House Concurrent Resolution 122 shall be considered as adopted.

SEC. 3. The chair of the Committee on Appropriations may insert in the Congressional Record at any time during the remainder of the second session of the 113th Congress such material as he may deem explanatory of the Senate amendment and the motion specified in the first section of this resolution.

SEC. 4. The requirement of clause 6(a) of rule XIII for a two-thirds vote to consider a report from the Committee on Rules on the same day it is presented to the House is waived with respect to any resolution reported through the legislative day of December 12, 2014.

The SPEAKER pro tempore. The gentleman from Oklahoma is recognized for 1 hour.

Mr. COLE. Mr. Speaker, for the purpose of debate only, I yield the customary 30 minutes to my good friend,