is obligation, as the people's elected representatives, to do everything we can to protect them from harm's way.

This measure passed the House in July by voice vote.

I backed the House-version of this measure because the bill will solve the personnel surety issue by allowing workers who have TWIC or HME cards to have access to chemical facilities without having to get another federal credential.

This is important to my constituents who already have TWIC cards and work in our petrochemical plants and drive the trucks to deliver raw materials and products they produce.

I am supportive of some of the changes the Senate made to this legislation. In particular, I am supportive of measures that will add greater worker participation into plant security plans and provide greater whistleblower protections for plant employees who want to report unsafe conditions at a plant.

I do have some concerns with allowing smaller facilities to self-certify, as added in by the Senate, because even smaller facilities, as we have unfortunately seen in Texas in recent years, can be dangerous and the American people deserve full assurance that facilities near them are safe.

Nonetheless, the underlining legislation is still sound and needs to be enacted. I urge my colleagues to join DHS Secretary Jeh Johnson, and impacted stakeholders and vote in support of the Senate amendments to H.R. 4007.

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. 4007.

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.

## CRITICAL INFRASTRUCTURE RESEARCH AND DEVELOPMENT ADVANCEMENT ACT OF 2014

Mr. MEEHAN. Mr. Speaker, I move to suspend the rules and concur in the Senate amendments to the bill (H.R. 2952) to amend the Homeland Security Act of 2002 to make certain improvements in the laws relating to the advancement of security technologies for critical infrastructure protection, and for other purposes.

The Clerk read the title of the bill.

The text of the Senate amendments is as follows:

Senate amendments:

Strike all after the enacting clause and insert the following:

***SECTION 1. SHORT TITLE.***

*This Act may be cited as the ''Cybersecurity Workforce Assessment Act''.*

***SEC. 2. DEFINITIONS.***

*In this Act—*

*(1) the term ''Cybersecurity Category'' means a position's or incumbent's primary work function involving cybersecurity, which is further defined by Specialty Area;*

*(2) the term ''Department'' means the Department of Homeland Security;*

*(3) the term ''Secretary'' means the Secretary of Homeland Security; and*

*(4) the term ''Specialty Area'' means any of the common types of cybersecurity work as recognized by the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework report.*

***SEC. 3. CYBERSECURITY WORKFORCE ASSESSMENT AND STRATEGY.***

*(a) WORKFORCE ASSESSMENT.—*

*(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, and annually thereafter for 3 years, the Secretary shall assess the cybersecurity workforce of the Department.*

*(2) CONTENTS.—The assessment required under paragraph (1) shall include, at a minimum—*

*(A) an assessment of the readiness and capacity of the workforce of the Department to meet its cybersecurity mission;*

*(B) information on where cybersecurity workforce positions are located within the Department;*

*(C) information on which cybersecurity workforce positions are—*

*(i) performed by—*

*(I) permanent full-time equivalent employees of the Department, including, to the greatest extent practicable, demographic information about such employees;*

*(II) independent contractors; and*

*(III) individuals employed by other Federal agencies, including the National Security Agency; or*

*(ii) vacant; and*

*(D) information on—*

*(i) the percentage of individuals within each Cybersecurity Category and Specialty Area who received essential training to perform their jobs; and*

*(ii) in cases in which such essential training was not received, what challenges, if any, were encountered with respect to the provision of such essential training.*

*(b) WORKFORCE STRATEGY.—*

*(1) IN GENERAL.—The Secretary shall—*

*(A) not later than 1 year after the date of enactment of this Act, develop a comprehensive workforce strategy to enhance the readiness, capacity, training, recruitment, and retention of the cybersecurity workforce of the Department; and*

*(B) maintain and, as necessary, update the comprehensive workforce strategy developed under subparagraph (A).*

*(2) CONTENTS.—The comprehensive workforce strategy developed under paragraph (1) shall include a description of—*

*(A) a multi-phased recruitment plan, including with respect to experienced professionals, members of disadvantaged or underserved communities, the unemployed, and veterans;*

*(B) a 5-year implementation plan;*

*(C) a 10-year projection of the cybersecurity workforce needs of the Department;*

*(D) any obstacle impeding the hiring and development of a cybersecurity workforce in the Department; and*

*(E) any gap in the existing cybersecurity workforce of the Department and a plan to fill any such gap.*

*(c) UPDATES.—The Secretary submit to the appropriate congressional committees annual updates on—*

*(1) the cybersecurity workforce assessment required under subsection (a); and*

*(2) the progress of the Secretary in carrying out the comprehensive workforce strategy required to be developed under subsection (b).*

***SEC. 4. CYBERSECURITY FELLOWSHIP PROGRAM.***

*Not later than 120 days after the date of enactment of this Act, the Secretary shall submit to the appropriate congressional committees a report on the feasibility, cost, and benefits of establishing a Cybersecurity Fellowship Program to offer a tuition payment plan for individuals pursuing undergraduate and doctoral degrees who agree to work for the Department for an agreed-upon period of time.*

Amend the title so as to read: ''An Act to require the Secretary of Homeland Security to assess the cybersecurity workforce of the Department of Homeland Security and develop a comprehensive workforce strategy, and for other purposes.''.

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

The Chair recognizes the gentleman from Pennsylvania.

GENERAL LEAVE

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

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

There was no objection.

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

Mr. Speaker, I rise in support of H.R. 2952, the Cybersecurity Workforce Assessment Act. H.R. 2952 was originally passed by the House as the Critical Infrastructure Research and Development Act of 2014. The updated legislation passed this week by our Senate colleagues adds important cybersecurity workforce provisions to the bill from what is known as McCaul-Meehan, H.R. 3696.

As cyber attacks by hackers from around the world grow increasingly sophisticated, it is more urgent than ever to improve our ability to stop them. Currently, the Department of Homeland Security's National Cybersecurity Communications and Integration Center, NCCIC, must compete with big technology companies and cybersecurity firms for cybersecurity workforce, while DHS is limited in its ability to attract talented and well-trained cyber warriors.

H.R. 2952 will require the Secretary to assess the cybersecurity workforce currently in DHS and develop a strategy to enhance it. The assessment would look at cyber positions, readiness, training, types of positions, and its ability to carry out its cyber mission, with the ultimate goal of enhancing these capabilities and produce a recruitment and implementation plan. Finally, the bill also requires the Secretary to submit a report on the feasibility of establishing a cybersecurity fellowship program.

This legislation along with the others we have brought up today are important pieces in improving the overall capabilities of the Department of Homeland Security and its ability to carry out its cybersecurity mission. This is a critically important piece of legislation which enables the Department of Homeland Security to compete for what are very, very in-demand individuals with talent in the area of cybersecurity and protections.

Most significantly, it allows us to have the kinds of quality of individuals who can work in an equal capacity

with the best of those who are in our other governmental institutions, and particularly those who are now working in the private sector. I believe that the capacity for DHS to attract these workers is critical to its mission. I continue to encourage the growth and development of that expertise.

I reserve the balance of my time.

□ 1000

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 H.R. 2952 that attaches the Cybersecurity Workforce Assessment Act.

For the Department of Homeland Security to be effective in its cybersecurity mission, it must have a workforce in place to meet this challenge. Yesterday, the House considered legislation to grant DHS special hiring authority to secure talent in the competitive cybersecurity employment marketplace.

The measure before you today includes language, authored by the gentlewoman from New York (Ms. CLARKE), that requires DHS to develop and issue a comprehensive workforce strategy for the Department's cybersecurity missions, and includes a 5-year implementation plan and a 10-year projection of the cybersecurity workforce needs of the Department.

Cybersecurity is a complex mission for the Department and requires a wide range of talent at all levels. Given the urgent nature of DHS' recruitment efforts, it is essential that the Department have this strategy in place.

Secondly, the bill requires the Department to assess the readiness and capacity of its workforce to meet its cybersecurity missions.

Lastly, the urgent need to fill critical national security positions often leads to an overreliance on contractors.

To encourage students to come to work for the government in this vital arena, this legislation also directs DHS to develop a plan to create a cybersecurity fellowship program. Under such a program, DHS would pay a promising student's tuition in exchange for a commitment to serve for a fixed period of time at the Department in a cybersecurity position.

For all these reasons, I urge my colleagues to vote for H.R. 2952, and I reserve the balance of my time.

Mr. MEEHAN. Mr. Speaker, I have no more speakers, and I am prepared to close once the gentleman does.

I reserve the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Speaker, I yield 3 minutes to the gentlewoman from New York (Ms. CLARKE), the ranking member of the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, who actually—this legislation is what she has been about.

Ms. CLARKE of New York. Mr. Speaker, I thank the gentleman for yielding time.

Mr. Speaker, I rise in support of the Senate amendment to H.R. 2952.

As my ranking member, Mr. THOMPSON, has said, for the Department of Homeland Security to be effective in its cybersecurity mission, it must have a workforce in place to meet this challenge. A longstanding interest of mine has been how best to help DHS meet its cyber workforce needs.

To that end, I have authored legislation that the committee unanimously approved in October to help ensure that DHS has the ''boots on the ground'' it needs to meet its diverse cybersecurity mission.

I would like to thank Chairman MEEHAN for the support you have shown for my efforts and the spirit of collaboration that you have shown.

This legislation requires DHS to develop and issue a comprehensive workforce strategy for the Department's cybersecurity missions. The Department is required to develop a 5-year implementation plan for that strategy and a 10-year projection of the cybersecurity workforce needs of the Department.

Before developing a strategy and implementation plan, it is important that DHS conduct a workforce assessment to get a sense of the readiness and capacity of the Department's cyber workforce.

It is also important that the Department determine where these positions are located within the Department and whether these positions are filled by permanent employees, independent contractors, detailees from other Federal agencies, or are vacant.

The workforce assessment required under this bill requires DHS to do just that.

Finally, I am glad that it directs DHS to develop a plan to establish a cybersecurity fellowship program under which talented undergraduates and doctoral candidates who sign on to work for the Department for an agreed-upon period would be provided tuition assistance.

Establishment of just such a program could help encourage students to come to work for the government in this vital arena.

I urge all of my colleagues to vote for the Senate amendment to H.R. 2952.

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

In closing, the legislation under consideration today is a product of bipartisan, bicameral negotiations. It has two parts: the core bill, which addresses the overall direction of Federal physical security and cybersecurity technology research and development efforts for protecting critical infrastructure; and the Clarke cybersecurity workforce amendment.

The language in both parts went through regular order and was approved by the House.

Therefore, I urge passage of H.R. 2952.

Before I yield back, in case Ms. CLARKE leaves, our committee has the unfortunate task next year of losing the chair and ranking member of this fine subcommittee, and I want to personally say that I really appreciate the manner in which they worked together on not just hearings but bringing forth good legislation to the full committee and, ultimately, this legislation we are dealing with today. So, I compliment both of them and we will miss them.

I yield back the balance of my time.

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

I want to thank the gentleman for his kind words and for his cooperation. The ranking member helped to set a tone for the collaboration on the committee, along with the leadership of our chairman of the committee, the gentleman from Texas. From the beginning, our focus was on working together to find solutions to the important issues which don't have a Democrat or a Republican unique perspective. It is an American perspective for us to put the priority on protecting our homeland.

I want to particularly express my appreciation to the ranking member of our subcommittee, the gentlewoman from New York, for all of her collaboration and the delightful manner in which we had to work through difficult issues together but, ultimately, got to compromise into important resolutions on these issues and matters of importance.

I appreciate her foresight on this particular provision, which I am pleased to strongly endorse. The reason for that is we are facing a very challenging time globally with the issue of cybersecurity. We not only have to worry about the impacts that can happen with cyber issues for the kinds of materials that we have got in the private sector, that they can be impacted, but we are also dealing in a very unsafe world in which threats are not only the theft of information or interference with systems, but the ability now for those who want to do us harm to use the cyber network to carry out that harm. Therefore, it is more critical than ever that we are able to attract to the Department of Homeland Security, in fact into government, the kinds of people who are prepared to be on the front lines of this battle.

This is exactly what this provision will enable us to do—first, to attract people, and I am always inspired by them, because they have the same sense and focus of dedication to their country that so many brave men and women who sign up and serve us in uniform. While they are serving in a different capacity, their service to our Nation is every bit as real in the sense of the personal sacrifice that they make to help us attract the best and the brightest to protect our assets. You have to appreciate that many of them, once they get that expertise, are very, very desirable to corporations and others in the business world who will pay them significantly more to come to work for them.

So this idea of beginning to create the bullpen, so to speak, of the next

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.''.