I encourage my colleagues to vote in favor of H.R. 3696.

Mr. THOMPSON of Mississippi. Mr. Speaker, I am pleased to be here today as an original cosponsor of this legislation, the National Cyber Security and Critical Infrastructure Protection Act.

This bipartisan legislation gives the Department of Homeland Security Congressional Authority to more fully carry out its civilian cyber mission, and to increase protection for our national critical infrastructure.

Importantly, this legislation also gives the Committee on Homeland Security a robust oversight position to make sure the Department carries out an innovative and cooperative relationship with industry, to protect the nation's privately owned critical infrastructure.

By giving DHS specific civilian authorities, it codifies what the President has already set into motion with his Cyber Executive Order 13636, issued in February of 2013, but Executive Authority goes only so far, and the President has said that his efforts cannot take the place Congressional action.

Mr. Speaker, we have stepped up to the plate. The legislation that Mr. MCCAUL and I worked on together, directs Federal agencies and private industry to coordinate the development and implementation of voluntary risk-based security standards, and codifies the ongoing process that the National Institute of Standards and Technology (NIST) and private industry have taken on.

We are asking that business and government find an adaptable and cooperative cyber security framework, for both government and private companies, not an off-the-shelf, or check-the-box solution.

We must depend on strong private sector leadership and accountability to focus on our nation's most pressing cyber vulnerabilities, protecting critical systems that when disrupted could cause catastrophic damage to our citizens. I believe this legislation will allow that process to move forward.

The President said it best, ''It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy and civil liberties.''

Critical infrastructure provides the essential services that underpin American society, and I suggest that the owners and operators of America's critical infrastructure are in a unique position to manage their own business risks with the help of civilian government agencies, to develop operational approaches that can make our critical infrastructure protected and durable.

Mr. Speaker, I have worked long and hard with the chairman to hammer out privacy and liability concerns held by myself, and many others, on both sides of the aisle.

There are no broad exceptions to the current privacy laws in this legislation, and it focuses on information sharing using existing structures. In fact, the ACLU commended the construction of this legislation by saying, ''. . . it is both pro-security and pro-privacy . . .''

We still have much work to do to achieve a higher level of cyber security in this country, and internationally.

We must approach the cyber threat arena in a way that is consistent with traditional American values, and by leading on the issue of respecting personal privacy in the efforts to achieve cyber security, we must continue to respect the safeguards for our constitutional right of freedom of speech.

The wrong way is to assume that we must cede all of our personal privacy and freedoms to remain safe.

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, H.R. 3696, as amended.

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

A motion to reconsider was laid on the table.

CRITICAL INFRASTRUCTURE RESEARCH AND DEVELOPMENT ADVANCEMENT ACT OF 2013

Mr. MEEHAN. Mr. Speaker, I move to suspend the rules and pass 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, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 2952

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 ''Critical Infrastructure Research and Development Advancement Act of 2013'' or the ''CIRDA Act of 2013''.

SEC. 2. DEFINITIONS.

Section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101) is amended by redesignating paragraphs (15) through (18) as paragraphs (16) through (19), respectively, and by inserting after paragraph (14) the following:

''(15) The term 'Sector Coordinating Council' means a private sector coordinating council that is—

''(A) recognized by the Secretary as such a Council for purposes of this Act; and

''(B) comprised of representatives of owners and operators of critical infrastructure within a particular sector of critical infrastructure.''.

SEC. 3. CRITICAL INFRASTRUCTURE PROTECTION RESEARCH AND DEVELOPMENT.

(a) STRATEGIC PLAN; PUBLIC-PRIVATE CONSORTIUMS.—

(1) IN GENERAL.—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:

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

''(a) IN GENERAL.—Not later than 180 days after the date of enactment of the Critical Infrastructure Research and Development Advancement Act of 2013, the Secretary, acting through the Under Secretary for Science and Technology, shall transmit 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. Once every 2 years after the initial strategic plan is transmitted to Congress under this section, the Secretary shall transmit to Congress an update of the plan.

''(b) CONTENTS OF PLAN.—The strategic plan 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 the Sector Coordinating Councils; and

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

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

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

''(B) emphasizes research and development of those 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. The initiatives shall consider 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 transmitted under this section.

''(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) the critical infrastructure Sector Coordinating Councils;

''(2) to the extent practicable, subject matter experts on critical infrastructure protection from universities, colleges, including historically black colleges and universities, Hispanic- serving institutions, and tribal colleges and universities, national laboratories, and private industry;

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

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

''SEC. 319. REPORT ON PUBLIC-PRIVATE RESEARCH AND DEVELOPMENT CONSORTIUMS.

''(a) IN GENERAL.—Not later than 180 days after the enactment of the Critical Infrastructure Research and Development Advancement Act of 2013, the Secretary, acting through the Under Secretary for Science and Technology, shall transmit to Congress a report on the Department's utilization of public-private research and development consortiums for accelerating technology development for critical infrastructure protection. Once every 2 years after the initial report is transmitted to Congress under this section, the Secretary shall transmit to Congress an update of the report. The report shall focus on those aspects of critical infrastructure protection that are predominately operated by the private sector and that would most benefit from rapid security technology advancement.

''(b) CONTENTS OF REPORT.—The report shall include—

''(1) a summary of the progress and accomplishments of on-going consortiums for critical infrastructure security technologies;

''(2) in consultation with the Sector Coordinating Councils and, to the extent practicable,

in consultation with subject-matter experts on critical infrastructure protection from universities, colleges, including historically black colleges and universities, Hispanic-serving institutions, and tribal colleges and universities, national laboratories, and private industry, a prioritized list of technology development focus areas that would most benefit from a public-private research and development consortium; and

''(3) based on the prioritized list developed under paragraph (2), a proposal for implementing an expanded research and development consortium program, including an assessment of feasibility and an estimate of cost, schedule, and milestones.''.

(2) LIMITATION ON PROGRESS REPORT REQUIREMENT.—Subsection (b)(5) of section 318 of the Homeland Security Act of 2002, as amended by paragraph (1) of this subsection, shall not apply with respect to the first strategic plan transmitted under that section.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding at the end of the items relating to such title the following:

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

''Sec. 319. Report on public-private research and development consortiums.''.

(c) CRITICAL INFRASTRUCTURE PROTECTION TECHNOLOGY CLEARINGHOUSE.—Section 313 of the Homeland Security Act of 2002 (6 U.S.C. 193) is amended by redesignating subsection (c) as subsection (d), and by inserting after subsection (b) the following:

''(c) CRITICAL INFRASTRUCTURE PROTECTION TECHNOLOGY CLEARINGHOUSE.—

''(1) DESIGNATION.—Under the program required by this section, the Secretary, acting through the Under Secretary for Science and Technology, and in coordination with the Under Secretary for the National Protection and Programs Directorate, shall designate a technology clearinghouse for rapidly sharing proven technology solutions for protecting critical infrastructure.

''(2) SHARING OF TECHNOLOGY SOLUTIONS.—Technology solutions shared through the clearinghouse shall draw from Government-furnished, commercially furnished, and publically available trusted sources.

''(3) TECHNOLOGY METRICS.—All technologies shared through the clearinghouse shall include a set of performance and readiness metrics to assist end-users in deploying effective and timely solutions relevant for their critical infrastructures.

''(4) REVIEW BY PRIVACY OFFICER.—The Privacy Officer of the Department appointed under section 222 shall annually review the clearinghouse process to evaluate its consistency with fair information practice principles issued by the Privacy Officer.''.

(d) EVALUATION OF TECHNOLOGY CLEARINGHOUSE BY GOVERNMENT ACCOUNTABILITY OFFICE.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall conduct an independent evaluation of, 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, the effectiveness of the clearinghouses established and designated, respectively, under section 313 of the Homeland Security Act of 2002, as amended by this section.

SEC. 4. NO ADDITIONAL AUTHORIZATION OF APPROPRIATIONS.

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

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Pennsylvania (Mr. MEEHAN) and the gentlewoman from New York (Ms. CLARKE) 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 have 5 legislative days within which to revise and extend their remarks and include any 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 as much time as I may consume.

Mr. Speaker, I rise in support of H.R. 2952, the Critical Infrastructure Research Development Advancement, or what we call the CIRDA, Act.

This legislation was passed out of full committee with unanimous bipartisan support, and I would like to thank my good friend, the ranking member on the Cybersecurity, Infrastructure Protection, and Security Technologies Committee, Ms. CLARKE, for cosponsoring and supporting this legislation.

One of the committee's most important duties is to protect our Nation's critical infrastructure. The CIRDA Act will change the way the Department of Homeland Security develops protections for critical infrastructure by creating and facilitating access to new and existing technologies.

Currently, there are barriers within the Department that inhibit strategizing for and, ultimately, the purchasing of the best tools that our country has to offer. The CIRDA Act will direct DHS to facilitate the development of a research and development strategy for critical infrastructure security technologies as well as explore the feasibility of expanding use of public-private R&D consortiums.

Our Nation must have access to new security technologies, and a public-private partnership can help spur innovation and economic competitiveness for entities that protect our Nation's defense systems, essential networks, Americans' financial information, chemical facilities, and the many other areas of our economy that are vital for the protection and confidence of Americans and our way of life.

This is critically important, Mr. Speaker, because of the fact of the nature, when we are dealing with cyber, what we are dealing with is not just the ability of what we can do today to create a defense, but the recognition of those on the other side who are looking to try to exploit our defenses. It is a constant chess game that is taking place.

Whatever we are able to do, immediately somebody is looking for a way to try to get around those protections and compromise them. As a result, we have to be able to have the best capacity, generated either in the private sector or in the government sector, and the ability to get those best protections to the places where they need to be the quickest and the most efficiently.

Finally, the legislation will designate a ''Technology Clearinghouse,'' where proven security tools can be rapidly shared among government and private partners. Keeping pace with the rapidly evolving variables of the threat to our Nation and the technological achievements only enhances our ability to combat attacks to the U.S.' critical infrastructure.

I urge support for the CIRDA Act.

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

CONGRESS OF THE UNITED STATES,
HOUSE OF REPRESENTATIVES, COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, DC, January 8, 2014.

Hon. MICHAEL MCCAUL,
Chairman, Committee on Homeland Security, Washington, DC.

DEAR CHAIRMAN MCCAUL: I am writing to you concerning the jurisdictional interest of the Committee on Science, Space, and Technology in H.R. 2952, the ''Critical Infrastructure Research and Development Advancement Act of 2013.'' The bill contains provisions that fall within the jurisdiction of the Committee on Science, Space, and Technology.

I recognize and appreciate the desire to bring this legislation before the House of Representatives in an expeditious manner, and accordingly, I will waive further consideration of this bill in Committee, notwithstanding any provisions that fall within the jurisdiction of the Committee on Science, Space, and Technology. This waiver, of course, is conditional on our mutual understanding that agreeing to waive consideration of this bill should not be construed as waiving, reducing, or affecting the jurisdiction of the Committee on Science, Space, and Technology.

This waiver is also given with the understanding that the Committee on Science, Space, and Technology will be added as a recipient of the report required to be provided by the General Accounting Office in Section 3 of the bill.

Additionally, the Committee on Science, Space, and Technology expressly reserves its authority to seek conferees on any provision within its jurisdiction during any House-Senate conference that may be convened on this, or any similar legislation. I ask for your commitment to support any request by the Committee for conferees on H.R. 2952 as well as any similar or related legislation.

I ask that a copy of this letter and your response be included in the report on H.R. 2952 and also be placed in the Congressional Record during consideration of this bill on the House floor.

Sincerely,

LAMAR SMITH,
Chairman, Committee on Science, Space, and Technology.

Enclosure.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC, January 8, 2014.

Hon. LAMAR SMITH,
Chairman, Committee on Science, Space, and Technology, Washington, DC.

DEAR CHAIRMAN SMITH: Thank you for your letter regarding H.R. 2952, the ''Critical Infrastructure Research and Development Act of 2013.'' I acknowledge that by forgoing a sequential referral on this legislation, your Committee is not diminishing or altering its jurisdiction.

I also concur with you that forgoing action on this bill does not in any way prejudice the Committee on Science, Space, and Technology with respect to its jurisdictional prerogatives on this bill or similar legislation in the future, and I would support your effort to seek appointment of an appropriate number of conferees to any House-Senate conference involving this legislation. In addition, the Committee on Science, Space, and Technology will be added as a recipient of the report provided by the General Accountability Office, required by Section 3 of this legislation, in the final version of text voted on by the full House.

Finally, I will include your letter and this response in the report accompanying H.R. 2952 as well as the Congressional Record during consideration of this bill on the House floor. I appreciate your cooperation regarding this legislation, and I look forward to working with the Committee on Science, Space, and Technology as the bill moves through the legislative process.

Sincerely,

MICHAEL T. MCCAUL,
Chairman.

Ms. CLARKE of New York. Mr. Speaker, I rise in strong support of H.R. 2952, the Critical Infrastructure Research and Development Advancement Act, and I yield myself such time as I may consume.

Mr. Speaker, I would like to thank the gentleman from Pennsylvania (Mr. MEEHAN), the chairman of the Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee, for introducing this very vital legislation. I appreciate him working with me and the rest of the committee to bring a thoughtful and bipartisan bill to the floor today.

In May, the Department of Justice released the names of five members of the Chinese People's Liberation Army that are suspected of carrying out cyber attacks against American companies for over 8 years. These indictments underscore the significant cyber vulnerabilities that the Department of Homeland Security works to identify and to thwart.

Some of the Department's most important efforts are targeted at protecting our critical infrastructure systems, such as communication systems and the electric grid. These systems have complex technological components that Americans expect will function without a glitch.

To carry out this mission, DHS is constantly researching and developing new technologies and defenses to help protect our infrastructure. This R&D is extremely important to the safety of American infrastructure.

At the same time, Congress must do proper oversight to ensure that it is done in an effective and efficient and focused way. That is why I cosponsored this act, which requires DHS to have a research and development strategy for critical infrastructure protection. This strategy is to be focused on identifying the most immediate threats and then developing a comprehensive set of initiatives to address them. It directs DHS to employ public-private partnerships, intragovernmental collaboration, University Centers for Excellence, and national laboratory technology transfers to make sure that DHS is working with state-of-the-art researchers and facilities. This strategy will help DHS keep ahead of the rapidly evolving cybersecurity attack that we hear about each and every day.

I am confident that, with the focused measures set forth in this bill and increased attention to the importance of science and technology in our antiterrorism efforts, we can be better equipped to defend America's critical infrastructure.

Mr. Speaker, cyberterrorists and cyber criminals are constantly innovating. We must do more to protect against these threats and foster great resilience of critical infrastructure networks to such threats. H.R. 2952 will make sure that we fight the new threats of this era with the most advanced technology solutions.

I urge my colleagues to join me in supporting H.R. 2952, the CIRDA Act, and I thank the gentleman from Pennsylvania (Mr. MEEHAN) for making it possible for us to have this on the floor today and to bring this new piece of legislation to fruition.

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

Mr. MEEHAN. Mr. Speaker, I want to express as well, as I close, once again, my appreciation for the tremendous collaborative working relationship with my colleague, Ms. CLARKE, and her staff and the staffs from both committees who have worked extensively to put these bills in the position that they have.

It is a joy to be part of something here in this Congress in a bipartisan fashion, in which people are working together to solve problems that challenge us all.

In my closing, I will include in the RECORD a letter in support of H.R. 2952 that is written by the Security Industry Association. These are the folks that represent over 470 suppliers of electronic physical security and other kinds of solutions.

SECURITY INDUSTRY ASSOCIATION,
September 12, 2013.

Hon. PAT MEEHAN,
Chairman, House Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, House of Representatives, Washington, DC.

DEAR CHAIRMAN MEEHAN: The Security Industry Association (SIA) would like to express its strong support for H.R. 2952, the ''Critical Infrastructure Research and Development Act of 2013'' (CIRDA). SIA represents more than 470 suppliers of electronic physical security solutions and countless technology leaders who design and install the security systems that protect millions of Americans each day in our nation's cities and towns, schools, factories, government buildings, transportation systems, ports, and other components of critical infrastructure. Owners and operators of these facilities work closely with SIA members as trusted advisors to ensure that cutting edge security technology solutions are adopted to prevent crime and terrorist attack.

SIA believes the CIRDA legislation will help the U.S. Department of Homeland Security (DHS) set clear and measureable R&D priorities that will accelerate the development of cutting-edge security technologies to protect critical infrastructure. More specifically, we strongly support the provision of H.R. 2952 that will require the development of a R&D strategy by the DHS Science and Technology Directorate that draws upon the expertise of Sector Coordinating Councils to identify security risks and technology gaps. With this essential information, DHS will be in a better position to communicate with the private sector about the security technologies that are most needed to prevent emerging threats to our homeland. SIA is pleased to serve on the Emergency Services Sector Coordinating Council and would be pleased to identify Subject Matter Experts from our membership to contribute to the development of this proposed R&D strategy and the Critical Infrastructure Protection Technology Clearinghouse provided for in your legislation.

Thank you for your leadership in introducing this important piece of legislation. SIA appreciates the priority this legislation places upon public-private partnerships and we look forward to working with you to ensure swift passage of CIRDA this year.

Sincerely,

DONALD R. ERICKSON,
Chief Executive Officer.

Mr. MEEHAN. The essence of what this is is the recognition by those who are in the industry that the Department of Homeland Security needs to be able to set clear and measurable R&D priorities that will accelerate the development of cutting-edge security technologies to protect the critical infrastructure.

When we are out there so frequently, what we hear from people is the concern: I have been attacked. What do I do to protect myself? And they turn to the Department of Homeland Security for advice.

As I said at an earlier point, the reality is that, while the responsibility rests with the Department and in the government to be able to facilitate the protection of the homeland and our assets, the reality is that 90 percent of these assets are placed within the private sector, and it is, in fact, there where much of, as much of, in fact, maybe some of the most pioneering research and development is accomplished.

One of the other realities we face, and I think the gentlelady pointed to it so well, this concept of innovation, when we often think of innovation in a positive way. It usually is a positive thing. It means somebody is always thinking of a new and better way to accomplish a task.

But criminals do that, too, and so do those who want to do us harm; and no matter how good our protections are, there is the reality that somebody else, the moment that it goes online, is looking for a way to get around it. That means that we have to have the capacity to have the ability to work quickly and effectively; then, once those who are in a position to know what is best, to be able to communicate down the line. So not just the big company that is situated someplace in New York City, but the small manufacturer in the middle of Kansas who is

still worried about their R&D, can have access to the same kinds of protections.

This bill allows that kind of collaboration to take place, working through the clearinghouse in the Department of Homeland Security. That is why I think it is so important that we take this step forward. I urge all Members to join me in supporting this bill.

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

Mr. MCCAUL. Mr. Speaker, I rise today in support of H.R. 2952, the Critical Infrastructure Research and Development Advancement Act of 2013, sponsored by Chairman Meehan.

This legislation is vital in our nation's efforts to protect our critical infrastructure from attacks. The Department of Homeland Security has identified 16 sectors of the U.S. economy so vital, that disruption or destruction would result in catastrophic life-threatening or life-altering challenges. The CIRDA Act will assist the Department by encouraging the development and procurement of new technologies aimed at infrastructure protection.

I thank Chairman MEEHAN for his efforts in crafting thoughtful legislation that will enhance DHS' research and development tools, streamline its public-private coordination efforts, while ensuring that technological and product solutions are shared between the Department and its private sector partners.

This bill is a bipartisan effort that was passed out of both subcommittee and full committee by voice vote, and I thank the subcommittee Chairman and Ranking Member for their work.

I urge support for H.R. 2952.

Mr. THOMPSON of Mississippi. Mr. Speaker, I rise in strong support of H.R. 2952, the ''Critical Infrastructure Research and Development Advancement Act.''

H.R. 2952 requires the Department to have a well-developed Research and Development strategy to work in targeted ways to advance cybersecurity, particularly within the critical infrastructure sector.

Keeping pace with cybercriminals, hackers, and others who seek to exploit vulnerabilities in critical IT networks is a major challenge for the Federal government and its partners in the private sector.

Americans take for granted that when they flip a switch, their lights will come on, when they pick up a phone, there will be a ringtone and when they pick up their Smartphone, they will have a signal.

The reliability and functioning of these systems is dependent on computer systems, often Internet-based systems.

Recently, we have seen the damage that can be done when systems are breached. The database breach at Target, a major retailer, involved 70 million stolen records, which affected over a hundred million people.

The true cost of these kinds of breaches is almost unknowable because of the complexity of the crimes, and the sometimes-untraceable use of the stolen information.

What we do know is that hackers are breaching the networks of large corporate companies, gaining access to proprietary industry information, as well as consumer data.

The Department of Homeland Security is the lead Federal agency responsible for researching and developing more advanced and effective cybersecurity technologies to defend Americans from such attacks.

The legislation before us today creates a technology clearinghouse to help promote partnerships with laboratories and universities throughout the Nation for research on how to enhance not only the cyber but the physical of critical infrastructure.

I am pleased that it directs DHS to seek out new ways to better collaboration with its Centers of Excellence on this research.

I am confident that the teams at Jackson State University and Tougaloo College in Mississippi, which are part of the Centers of Excellence network, can make valuable contributions to this effort.

On a bipartisan basis, this Committee has developed a record for championing homeland security research and development while, at the same time, demanding accountability of DHS to ensure solid decision-making drives the expenditure of limited R&D dollars.

I urge my fellow colleagues to support H.R. 2952, the ''Critical Infrastructure Research and Development Advancement Act of 2013''.

Ms. JACKSON LEE. Mr. Speaker, I rise in support of H.R. 2952, a bill that will create a research and development strategy for critical infrastructure security technologies to protect critical American infrastructure from physical and cyber-attacks.

As a senior member of the Homeland Security Committee, I believe that the technology and protection of our critical infrastructure falls short in addressing the cyber-attacks we face on a daily basis.

We are in dire need of new security technologies to keep pace with rapidly evolving threats and the rapid advancement of the infrastructure itself.

This bill requires the Homeland Security Department to facilitate the development of a research and development (R&D) strategy for critical infrastructure security technologies.

The measure requires the Homeland Security Department, within 180 days of enactment and every two years thereafter, to submit to Congress a strategic plan for research and development efforts addressing the protection of critical infrastructure.

The plan must identify critical infrastructure security risks and any associated security technology gaps

The department also must submit a report to Congress, within 180 days of enactment and every two years thereafter, on departmental use of public-private consortiums to develop technology to protect such infrastructure.

The Congressional Budget Office (CBO) estimates that the bill would cost less than $500,000 annually in 2014 and 2015, assuming the availability of appropriated funds.

The bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would not affect the budgets of state, local or tribal governments.

Mr. Speaker, the cost of this bill is a small price to pay for the increased security and safety it will provide once it has been successfully implemented.

In closing, I would like to state that I have always advocated for strengthening our Department of Homeland Security and giving the department the proper tools to protect our country.

It is important that we continue to help support the agencies that protect us.

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 pass the bill, H.R. 2952, as amended.

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

A motion to reconsider was laid on the table.

□ 1730

HOMELAND SECURITY CYBERSECURITY BOOTS-ON-THE-GROUND ACT

Mr. MEEHAN. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3107) to require the Secretary of Homeland Security to establish cybersecurity occupation classifications, assess the cybersecurity workforce, develop a strategy to address identified gaps in the cybersecurity workforce, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3107

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

SECTION 1. HOMELAND SECURITY CYBERSECURITY WORKFORCE.

(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. 226. CYBERSECURITY OCCUPATION CATEGORIES, WORKFORCE ASSESSMENT, AND STRATEGY.

''(a) SHORT TITLE.—This section may be cited as the 'Homeland Security Cybersecurity Boots-on-the-Ground Act'.

''(b) CYBERSECURITY OCCUPATION CATEGORIES.—

''(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this section, the Secretary shall develop and issue comprehensive occupation categories for individuals performing activities in furtherance of the cybersecurity mission of the Department.

''(2) APPLICABILITY.—The Secretary shall ensure that the comprehensive occupation categories issued under paragraph (1) are used throughout the Department and are made available to other Federal agencies.

''(c) CYBERSECURITY WORKFORCE ASSESSMENT.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this section and annually thereafter, the Secretary shall assess the readiness and capacity of the workforce of the Department to meet its cybersecurity mission.

''(2) CONTENTS.—The assessment required under paragraph (1) shall, at a minimum, include the following:

''(A) Information where cybersecurity positions are located within the Department, specified in accordance with the cybersecurity occupation categories issued under subsection (b).

''(B) Information on which cybersecurity positions are—

''(i) performed by—

''(I) permanent full time departmental employees, together with demographic information about such employees' race, ethnicity, gender, disability status, and veterans status;

''(II) individuals employed by independent contractors; and