HONORING ZETA PHI BETA ON 100 YEARS

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

Mr. CARSON of Indiana. Mr. Speaker, I rise today to honor Zeta Phi Beta sorority on a century of nurturing leaders and improving communities.

Founded on Howard University's campus 100 years ago, Zeta has chartered hundreds of chapters worldwide and has a membership of 150,000. Its list of esteemed alumni is a who's who of Black excellence, including trailblazers in business, law, advocacy, public service, and more.

I am incredibly proud that my grandmother, Julia Carson, is a part of this amazing legacy of women.

As the sorority moves on to its next 100 years, I have no doubt that it will maintain and strengthen its zeal for excellence.

Once again, congratulations to Zeta Phi Beta on your first century of success.

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, the Chair will postpone further proceedings today on motions to suspend the rules on which the yeas and nays are ordered.

The House will resume proceedings on postponed questions at a later time.

ENERGY EMERGENCY LEADERSHIP ACT

Mr. PALLONE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 362) to amend the Department of Energy Organization Act with respect to functions assigned to Assistant Secretaries, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 362

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 ''Energy Emergency Leadership Act''.

SEC. 2. FUNCTIONS ASSIGNED TO ASSISTANT SECRETARIES.

(a) IN GENERAL.—Subsection (a) of section 203 of the Department of Energy Organization Act (42 U.S.C. 7133(a)) is amended by adding at the end the following new paragraph:

''(12) Energy emergency and energy security functions, including—

''(A) responsibilities with respect to infrastructure, cybersecurity, emerging threats, supply, and emergency planning, coordination, response, and restoration; and

''(B) upon request of a State, local, or tribal government or energy sector entity, and in consultation with other Federal agencies as appropriate, provision of technical assistance, support, and response capabilities with respect to energy security threats, risks, and incidents.''.

(b) COORDINATION.—The Secretary of Energy shall ensure that the functions of the Secretary described in section 203(a)(12) of the Department of Energy Organization Act (as added by this Act) are performed in coordination with relevant Federal agencies.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from New Jersey (Mr. PALLONE) and the gentleman from Oregon (Mr. WALDEN) each will control 20 minutes.

The Chair recognizes the gentleman from New Jersey.

GENERAL LEAVE

Mr. PALLONE. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and include extraneous material on H.R. 362.

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

There was no objection.

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

Mr. Speaker, this legislation and the two bills that will follow it are bipartisan bills that will help protect our energy grid from cyberattacks.

In hearings before our Energy Subcommittee last year, we heard from the Federal Energy Regulatory Commission, or FERC, from the members of FERC, that our energy grid is being attacked each and every single day by state actors or their entities.

Former Energy Secretary Perry started to address this important issue by creating the Office of Cybersecurity, Energy Security, and Emergency Response, or CESER. He further enhanced its stature by making its leader an Assistant Secretary.

We agree with those decisions, and this legislation would help elevate the importance of this issue while putting Congress' bipartisan stamp of approval on these executive actions.

H.R. 362 would simply amend section 203(a) of the Department of Energy Organization Act by establishing a new assistant secretary position responsible for cybersecurity and emergency response issues.

The Department of Energy is the lead agency for ensuring the cybersecurity of the electric grid, and the newly created assistant secretary would have jurisdiction over all energy emergency and security functions related to energy supply, infrastructure, and cybersecurity.

This bill would also authorize the new assistant secretary to provide DOE technical assistance, as well as support and response capabilities with respect to energy security risks to State, local, or Tribal governments upon request.

The bill would also require the assistant secretary and the Department of Energy to coordinate with the Department of Homeland Security and other relevant Federal agencies in carrying out the bill's provisions.

This bill would go a long way, in my opinion, in helping to protect the Nation's electric infrastructure from hackers who would attempt to disrupt our energy grid and cause untold harm to our economy, our daily lives, and our overall national security.

Mr. Speaker, I want to commend Representatives WALBERG and Energy Subcommittee Ranking Member UPTON for their leadership and for working with Chairman RUSH and me on the Energy Emergency Leadership Act. I also want to thank Ranking Member UPTON and full Committee Ranking Member WALDEN for their ongoing partnership with us over the years on cybersecurity matters. That partnership was essential in getting these three critical bills to the floor today.

Mr. Speaker, I urge all of my colleagues to support this bipartisan bill, and I reserve the balance of my time.

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

Mr. Speaker, I, too, rise in support of H.R. 362, Energy Emergency Leadership Act.

Mr. Speaker, this legislation, sponsored by Representatives RUSH and WALBERG, strengthens the Department of Energy's important energy emergency mission. It does so by requiring the well-established energy emergency and cybersecurity functions at DOE to be organized under the leadership of an assistant secretary confirmed by the United States Senate.

Just over 2½ years ago, then-Secretary of the Department of Energy Rick Perry recognized the importance of elevating this mission within the Department, and he established an Assistant Secretary-led office, the Office of Cybersecurity, Energy Security, and Emergency Response. This office has proven its worth in various situations over the past 2 years, Mr. Speaker, including assistance relating to hurricanes and wildfires.

This bill would amend the Department of Energy Organization Act to establish in law and, therefore, maintain that a Senate-confirmed assistant secretary would lead the Department of Energy's emergency response and cybersecurity functions.

This legislation will ensure the Department has the focused and accountable leadership to more fully protect the public from fuel and electricity supply disruptions against all the hazards, natural or man-made, including emerging threats from our foreign adversaries to the Nation's electric grid.

The bill has been drafted to ensure the Department carries out its responsibilities in coordination with other agencies by improving coordination across the Department, ensuring more effective interagency collaborations, and increasing accountability to the Congress.

A vote for H.R. 362 is a vote for ensuring high-level leadership over energy emergencies at the Department of Energy for the benefit of public safety and welfare, and for stronger cybersecurity protections in the electricity systems.

Mr. Speaker, I urge support of the legislation, and I reserve the balance of my time.

Mr. PALLONE. Mr. Speaker, I yield such time as he may consume to the gentleman from Mississippi (Mr. THOMPSON), the chairman of the Committee on Homeland Security.

Mr. THOMPSON of Mississippi. Mr. Speaker, I rise for purposes of expressing my concerns with H.R. 362, H.R. 360, and H.R. 359, in their current forms.

Mr. Speaker, I am concerned that, without clarification, these bills risk significantly disrupting how the Federal Government has collaborated regarding cybersecurity for nearly two decades.

Congress has repeatedly supported the framework that designates the Department of Homeland Security as the lead for ensuring that Federal agencies work together and with the private sector to protect and secure critical infrastructure.

This framework was developed in the wake of the 9/11 terrorist attacks to guard against repeating the mistakes of a disjointed, siloed approach to national security and is well-understood and has been well-litigated within this body.

It has been reinforced repeatedly by numerous laws, Presidential policy directives, and executive orders that have the support of Democrats and Republicans alike.

□ 1215

The policy is clear: DHS serves as the lead agency responsible for coordinating Federal efforts to protect critical infrastructure in the 16 diverse sectors.

To carry out this mission, DHS, through the Cybersecurity and Infrastructure Security Agency, or CISA, is tasked with coordinating with other sector-specific agencies.

The Department of Energy is the sector-specific agency for the energy sector and is well-suited to do so. Its role as the facilitator of robust cybersecurity within the energy sector is important.

However, the problem common to the three measures today is that, in their current forms, they risk siloing cybersecurity efforts when it comes to protecting the energy sector, as none of them acknowledges DHS as the coordinating partner to DOE for cybersecurity.

As a reminder, this is the same infrastructure that has been under sustained, sophisticated attack from foreign adversaries, some of which have been successful.

While cyberattacks against the energy sector have accelerated, the sector does not exist in a vacuum. Over the past few years, DHS and the FBI have been sounding the alarm about Russian-led attacks on energy infrastructure that coincide with and often mirror attacks in other sectors.

In a 2018 technical alert issued to all infrastructure sectors, DHS and the FBI described a multistage intrusion campaign by the Kremlin. The alert explained that Russia used a similar playbook to target U.S. entities as well as organizations in the energy, nuclear, commercial facility, water, aviation, and commercial manufacturing sectors.

In the face of these threats, the Cybersecurity Solarium Commission and others have called for a redoubling of efforts to strengthen DHS' role.

I would like to enter into a colloquy with the gentleman from New Jersey.

Chairman PALLONE, I remain concerned that the cyber bill before us, as well as the other cybersecurity bills being considered today, do not provide sufficient direction to the Secretary of Energy to coordinate his Department's cybersecurity activities with the Department of Homeland Security.

Is it your intent that the activities authorized by this legislation be carried out in coordination with the Homeland Security Secretary and that Department?

Mr. PALLONE. Will the gentleman yield?

Mr. THOMPSON of Mississippi. I yield to the gentleman from New Jersey.

Mr. PALLONE. Yes, Mr. Speaker, it is absolutely my intent and the intent of the Energy and Commerce Committee that these bills be implemented in coordination with the Secretary and the Department of Homeland Security. In fact, the sole reason we are amending these bills is to make clear that the Department of Energy must implement these bills in coordination with other Federal agencies.

I want to make clear that we intend, first and foremost, DOE to coordinate with the Department of Homeland Security. We have made that clear to DOE at the highest levels, and the Department has acknowledged that it will coordinate with the Department of Homeland Security in implementing these bills.

Mr. THOMPSON of Mississippi. Mr. Speaker, I am glad to hear that, without any equivocation, Mr. PALLONE fully expects DOE to coordinate with DHS, but that only addresses one of my concerns.

My other concern is that these bills do not, in any way, shape, or form, detract from or erode the existing authorities of the Secretary and Department of Homeland Security, including the authorities set forth in the Cybersecurity and Infrastructure Security Act of 2018.

I understand that is your position that these bills do not in any way infringe on DHS' existing authorities or prerogatives. Is that correct?

Mr. PALLONE. If the gentleman continues to yield, yes, Chairman THOMPSON, it is correct, and I thank my friend, the chairman of the Homeland Security Committee, for that question and the opportunity to further clarify what these bills do and do not do.

These bills completely confine themselves to codifying or further specifying authorities and obligations the Secretary of Energy already has as the sector-specific agency for electricity under the FAST Act, the Federal Power Act, and the Department of Energy Organization Act.

So let me make this clear: Nothing in these bills is intended to infringe, curtail, or otherwise affect the authorities of the Department of Homeland Security as they exist at this moment. And I will go even further to say that nothing in these bills actually affects, in any way, shape, or form, the existing authorities or prerogatives of the Department of Homeland Security or its Secretary in any area. Any interpretation to the contrary is simply incorrect.

Mr. THOMPSON of Mississippi. Mr. Speaker, I thank my friend from New Jersey for that information.

To be clear, it is your intention that these measures do not affect DHS' authority under PPD–21, PPD–41, Executive Order 13691, and Executive Order 13636?

Mr. PALLONE. If the gentleman continues to yield, that is correct, Mr. Chairman.

Mr. THOMPSON of Mississippi. Would you agree to work with me to communicate to the Senate and the administration that the intention behind these measures is to have the Secretary of Energy coordinate activities with DHS consistent with the existing cybersecurity framework?

Mr. PALLONE. If the gentleman continues to yield, yes, and I would be pleased to do so.

Mr. THOMPSON of Mississippi. Mr. Speaker, I thank Mr. PALLONE for addressing my questions.

While I still have concerns over these measures, I appreciate his willingness to put into the RECORD these statements and look forward to working with him to clarify expectations going forward.

Mr. PALLONE. Mr. Speaker, I thank the gentleman and understand that he continues to have concerns, and I know I may not be able to address them all today, but I commit to working with my friend from Mississippi and my Republican colleagues to try to further address these concerns going forward.

Mr. THOMPSON of Mississippi. Mr. Speaker, I thank the gentleman from New Jersey for his cooperation and clarifying these three pieces of legislation.

Mr. WALDEN. Mr. Speaker, I hope my colleagues will join me and the chairman of the Energy and Commerce Committee in supporting passage of this legislation and our efforts to ensure that our electric grid and our power supply sources are safe and secure.

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

Mr. PALLONE. Mr. Speaker, I urge support for the legislation, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New Jersey (Mr.

PALLONE) that the House suspend the rules and pass the bill, H.R. 362, 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.

CYBER SENSE ACT OF 2020

Mr. PALLONE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 360) to require the Secretary of Energy to establish a voluntary Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 360

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 ''Cyber Sense Act of 2020''.

SEC. 2. CYBER SENSE.

(a) IN GENERAL.—The Secretary of Energy, in coordination with relevant Federal agencies, shall establish a voluntary Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system, as defined in section 215(a) of the Federal Power Act (16 U.S.C. 824o(a)).

(b) PROGRAM REQUIREMENTS.—In carrying out subsection (a), the Secretary of Energy shall—

(1) establish a testing process under the Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system, including products relating to industrial control systems and operational technologies, such as supervisory control and data acquisition systems;

(2) for products and technologies tested under the Cyber Sense program, establish and maintain cybersecurity vulnerability reporting processes and a related database;

(3) provide technical assistance to electric utilities, product manufacturers, and other electricity sector stakeholders to develop solutions to mitigate identified cybersecurity vulnerabilities in products and technologies tested under the Cyber Sense program;

(4) biennially review products and technologies tested under the Cyber Sense program for cybersecurity vulnerabilities and provide analysis with respect to how such products and technologies respond to and mitigate cyber threats;

(5) develop guidance, that is informed by analysis and testing results under the Cyber Sense program, for electric utilities for procurement of products and technologies;

(6) provide reasonable notice to the public, and solicit comments from the public, prior to establishing or revising the testing process under the Cyber Sense program;

(7) oversee testing of products and technologies under the Cyber Sense program; and

(8) consider incentives to encourage the use of analysis and results of testing under the Cyber Sense program in the design of products and technologies for use in the bulk-power system.

(c) DISCLOSURE OF INFORMATION.—Any cybersecurity vulnerability reported pursuant to a process established under subsection (b)(2), the disclosure of which the Secretary of Energy reasonably foresees would cause harm to critical electric infrastructure (as defined in section 215A of the Federal Power Act), shall be deemed to be critical electric infrastructure information for purposes of section 215A(d) of the Federal Power Act.

(d) FEDERAL GOVERNMENT LIABILITY.—Nothing in this section shall be construed to authorize the commencement of an action against the United States Government with respect to the testing of a product or technology under the Cyber Sense program.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from New Jersey (Mr. PALLONE) and the gentleman from Oregon (Mr. WALDEN) each will control 20 minutes.

The Chair recognizes the gentleman from New Jersey.

GENERAL LEAVE

Mr. PALLONE. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and include extraneous material on H.R. 360.

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

There was no objection.

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

Mr. Speaker, I rise in support of H.R. 360, the Cyber Sense Act of 2020.

Grid security is a national security issue and one that is clearly and properly delegated under law to the Secretary of Energy to manage together with the industry. We must give the electric sector the tools and technologies necessary to protect our grid from malicious harm.

Fortunately, there has not yet been a broad cyberattack that has taken down large parts of the grid in the United States, but we must not let our guard down.

H.R. 360 gives the Department of Energy important and new authorities to facilitate more secure technologies and equipment in our Nation's grid. It also now requires the Secretary to coordinate with the Department of Homeland Security and other relevant Federal agencies in order to ensure smooth and seamless implementation across the Federal Government.

This bill requires the Department of Energy to set up a voluntary Cyber Sense program to identify cyber-secure products that could be used in the bulk-power system.

This program would also provide technical assistance to electric utilities and product manufacturers to assist them in developing solutions to mitigate cyber vulnerabilities in the grid.

I thank my colleagues, Representative MCNERNEY and Representative LATTA, for their hard work on this critical issue. Their partnership and bipartisan leadership on cybersecurity matters continues to benefit us all.

Mr. Speaker, I urge my colleagues to support this important bill, and I reserve the balance of my time.

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

Mr. Speaker, H.R. 360, the Cyber Sense Act, was authored and introduced by my Energy and Commerce Committee colleagues, Mr. LATTA and Mr. MCNERNEY.

The bill was reported unanimously from the Energy and Commerce Committee to improve the cybersecurity of the supply chains for the components of our Nation's electricity infrastructure.

To ensure the security of our Nation's electricity grid means we must ensure bulk-power system components and technologies are not vulnerable to cyber threats and attacks.

This is especially important, given the threats our nation-state adversaries pose to the bulk-power and electric systems, as indicated by the President's May 1, 2020, executive order giving the Department of Energy authority to take action to protect the bulk-power system. This bill would help that effort.

H.R. 360 would establish a voluntary Department of Energy program that identifies and promotes cyber-secure products intended for use in the bulk-power system, including products related to industrial control systems.

The bill would authorize the Department of Energy to provide technical assistance to electric utilities, product manufacturers, and other electricity sector stakeholders to help mitigate identified cybersecurity vulnerabilities.

The bill also was amended to make clear these efforts of the Department of Energy would include, as appropriate, other relevant Federal agencies like the Department of Homeland Security.

Mr. Speaker, a vote for H.R. 360 is a vote for providing an important new tool to electric utility supply chains from cybersecurity threats. I urge support of the legislation, and I reserve the balance of my time.

Mr. PALLONE. Mr. Speaker, I yield such time as he may consume to the gentleman from California (Mr. MCNERNEY).

Mr. MCNERNEY. Mr. Speaker, for lawmakers to encourage and enable innovative advancements that can improve the security and reliability of our Nation's energy grid, we must work on a bipartisan basis, as the bills under consideration show.

Fortunately, the modernization and innovation of our Nation's energy infrastructure is already under way. What was once a one-way delivery system has evolved into a dynamic network where information and energy flow both ways.

Technological advancements are also born from the need to secure the energy grid against potential physical and cyber threats. For example, the technology allowing for the rerouting of power and quick response in the event of attacks is being deployed across the grid.

The cooperation among Federal, State, and local governments is essential to protecting Americans and our