from fuel and electricity supply disruptions against all 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 responsibility in coordination with other agencies by improving coordination across the Department; ensuring more effective interagency collaborations; and increasing accountability to Congress.

Establishing accountable leadership of this DOE mission is an important step in the face of increased threats, vulnerabilities, and interdependencies of energy infrastructure and end-use systems.

Protecting energy security requires defense in depth.

This means a strong energy sector, strong state capabilities, and ensuring sector agencies, like the Department of Energy, have the tools and accountable leadership they need to respond to energy emergencies.

A vote for H.R. 3119 is a vote for ensuring accountable DOE leadership over energy emergencies for the benefit of public safety and welfare and for stronger cybersecurity protections and energy systems.

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

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

Mr. LATTA. Mr. Speaker, I yield 5 minutes to the gentleman from Michigan (Mr. WALBERG), one of the coleads on this legislation.

□ 1415

Mr. WALBERG. Mr. Speaker, I thank my good friend for yielding and allowing me the opportunity to speak.

I rise today in support of H.R. 3119, the Energy Emergency Leadership Act. I thank my good friend from Illinois, Mr. BOBBY RUSH, for continuing to work with me to get this bill across the finish line.

This is the third Congress in a row that we have introduced this bill, each time passing the Committee on Energy and Commerce with unanimous, bipartisan support.

And frankly, given what we have seen just over the last few months in disruptions to our energy supply—including the Colonial Pipeline attack—it is well past due for this important energy security measure to be enacted in law.

Mr. Speaker, our Nation's economy and the health and safety of the American public depend upon the reliable and uninterrupted supply of fuels and electricity.

Hazards of all forms—including natural disasters, digital, and cyberattacks—are no longer just threats. They are occurring at an alarming and continuing rate.

Whether it is power outages in Texas and California due to weather events, or foreign adversaries hacking into our pipelines or grid, it is critical that we better equip our Federal agencies to prevent and respond to attacks in a way that fully protects the public.

Presidential administrations of both parties have recognized this by providing the Department of Energy with the responsibilities, expertise, and tools to ensure the reliable supply of energy.

It is time Congress does its part by requiring the energy emergency and cybersecurity functions at DOE to be organized under the leadership of an assistant secretary confirmed by the Senate. This will ensure the Department has focused and accountable leadership with high-level continuity throughout future administrations.

H.R. 3119 will encourage more effective and seamless information-sharing with Federal and industry stakeholders on energy security threats, risks, and incidents, as well as recovery and response.

Mr. Speaker, I urge my colleagues to vote in favor of H.R. 3119 in order to protect our Nation's electric infrastructure from foreign adversaries who are attempting to disrupt our energy system and cause untold harm to our economy, our daily lives, and our national security.

Mr. LATTA. Mr. Speaker, I am prepared to close, and I yield myself such time as I may consume.

Mr. Speaker, I again thank Representative WALBERG and Representative BOBBY RUSH for their work on this very important legislation because, again, it is going to ensure that the Department of Energy has the focus and the accountable leadership to more fully protect the public from any electricity fuel supply disruptions against all hazards—natural or manmade—including emerging threats from our foreign adversaries to our Nation's electric grid.

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

Mr. PALLONE. Mr. Speaker, I thank both sides of the aisle, Mr. LATTA and others, for their help in getting this bill moved.

Mr. Speaker, again, I would ask 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. 3119.

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.

ENHANCING GRID SECURITY THROUGH PUBLIC-PRIVATE PARTNERSHIPS ACT

Mr. PALLONE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 2931) to provide for certain programs and developments in the Department of Energy concerning the cybersecurity and vulnerabilities of, and physical threats to, the electric grid, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 2931

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 ''Enhancing Grid Security through Public-Private Partnerships Act''.

SEC. 2. PROGRAM TO PROMOTE AND ADVANCE PHYSICAL SECURITY AND CYBERSECURITY OF ELECTRIC UTILITIES.

(a) ESTABLISHMENT.—The Secretary of Energy, in coordination with relevant Federal agencies and in consultation with State regulatory authorities, industry stakeholders, and the Electric Reliability Organization, as the Secretary determines appropriate, shall carry out a program to—

(1) develop, and provide for voluntary implementation of, maturity models, self-assessments, and auditing methods for assessing the physical security and cybersecurity of electric utilities;

(2) provide training to electric utilities to address and mitigate cybersecurity supply chain management risks;

(3) increase opportunities for sharing best practices and data collection within the electric sector;

(4) assist with cybersecurity training for electric utilities;

(5) advance the cybersecurity of third-party vendors that work in partnerships with electric utilities; and

(6) provide technical assistance for electric utilities subject to the program.

(b) SCOPE.—In carrying out the program under subsection (a), the Secretary of Energy shall—

(1) take into consideration different sizes of electric utilities and the regions that such electric utilities serve;

(2) prioritize electric utilities with fewer available resources due to size or region; and

(3) to the extent practicable, utilize and leverage existing Department of Energy programs.

(c) PROTECTION OF INFORMATION.—Information provided to, or collected by, the Federal Government pursuant to this section—

(1) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code; and

(2) shall not be made available by any Federal, State, political subdivision or tribal authority pursuant to any Federal, State, political subdivision, or tribal law requiring public disclosure of information or records.

SEC. 3. REPORT ON CYBERSECURITY AND DISTRIBUTION SYSTEMS.

(a) IN GENERAL.—The Secretary of Energy, in coordination with relevant Federal agencies and in consultation with State regulatory authorities, industry stakeholders, and the Electric Reliability Organization, as the Secretary determines appropriate, shall submit to Congress a report that assesses—

(1) priorities, policies, procedures, and actions for enhancing the physical security and cybersecurity of electricity distribution systems to address threats to, and vulnerabilities of, such electricity distribution systems; and

(2) implementation of such priorities, policies, procedures, and actions, including an estimate of potential costs and benefits of such implementation, including any public-private cost-sharing opportunities.

(b) PROTECTION OF INFORMATION.—Information provided to, or collected by, the Federal Government pursuant to this section—

(1) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code; and

(2) shall not be made available by any Federal, State, political subdivision or tribal authority pursuant to any Federal, State, political subdivision, or tribal law requiring public disclosure of information or records.

SEC. 4. ELECTRICITY INTERRUPTION INFORMATION.

(a) INTERRUPTION COST ESTIMATE CALCULATOR.—The Secretary of Energy, in coordination with relevant Federal agencies and in consultation with State regulatory authorities, industry stakeholders, and the Electric Reliability Organization, as the Secretary determines appropriate, shall update the Interruption Cost Estimate Calculator, as often as appropriate and feasible, but not less than once every 2 years.

(b) INDICES.—The Secretary of Energy, in coordination with relevant Federal agencies and in consultation with State regulatory authorities, industry stakeholders, and the Electric Reliability Organization, as the Secretary determines appropriate, shall, as often as appropriate and feasible, update the following:

(1) The System Average Interruption Duration Index.

(2) The System Average Interruption Frequency Index.

(3) The Customer Average Interruption Duration Index.

(c) SURVEY.—The Administrator of the Energy Information Administration shall collect information on electricity interruption costs, if available, from a representative sample of owners of electric grid assets through a biennial survey.

SEC. 5. DEFINITIONS.

In the Act, the following definitions apply:

(1) ELECTRIC RELIABILITY ORGANIZATION.—The term ''Electric Reliability Organization'' has the meaning given such term in section 215(a)(2) of the Federal Power Act (16 U.S.C. 824o(a)(2)).

(2) ELECTRIC UTILITY.—The term ''electric utility'' has the meaning given such term in section 3 of the Federal Power Act (16 U.S.C. 796).

(3) STATE REGULATORY AUTHORITY.—The term ''State regulatory authority'' has the meaning given such term in section 3 of the Federal Power Act (16 U.S.C. 796).

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from New Jersey (Mr. PALLONE) and the gentleman from Ohio (Mr. LATTA) 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. 2931.

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 begin by thanking my colleagues on the Committee on Energy and Commerce, Representative MCNERNEY of California and Representative LATTA of Ohio, for their continued work and cooperation on energy security issues and for introducing H.R. 2931, the Enhancing Grid Security Through Public-Private Partnerships Act.

This legislation could not be more necessary. Our Nation is facing an increasing number of physical and cyber threats to its electric grid and infrastructure. This bill addresses those threats by directing the Secretary of Energy, in consultation with the Electric Reliability Organization, States, other Federal agencies, and industry stakeholders, to create and implement a program to enhance the physical and cybersecurity of electric utilities.

It calls for cybersecurity training to mitigate supply chain risks and improving the cybersecurity of third-party utility vendors. It also encourages utilities to share best practices and data within the electric sector.

The bill requires the Secretary of Energy to deliver a report to Congress on general cybersecurity concerns and to coordinate with the Department of Homeland Security and other relevant agencies to ensure good communications and smooth implementation of this program across the government.

Finally, the bill instructs the Secretary of Energy to update the Interruption Cost Estimate Calculator, which is an electric reliability planning tool for estimating electricity interruption costs and the benefits associated with reliability benefits.

Mr. Speaker, H.R. 2931 is an important bipartisan bill that will help address the security of our Nation's electric utilities, and I urge my colleagues to support it.

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

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

Mr. Speaker, I rise today in support of H.R. 2931, the first of two grid security bills I have worked closely on with my good friend and colleague, the gentleman from California (Mr. MCNERNEY) over the last several Congresses.

The goal of these two bills is to improve the resiliency of our Nation's energy grid against cyberattacks. Since the House last considered these bills on the floor, our country has experienced a new wave of cyberattacks on our critical infrastructure.

On December 13, 2020, the cybersecurity firm, FireEye, published research that a malicious actor was exploiting a supply chain vulnerability in SolarWinds products to hack into government and private sector information technology networks.

On May 8 of this year, the Colonial Pipeline Company announced that it was forced to halt its pipeline operation due to a ransomware attack, which disrupted critical supplies of gasoline and other refined products throughout the Southeast and the East Coast.

Cyberattacks on our critical infrastructure will only continue to grow in both size and severity and Congress must take a stand. H.R. 2931, the Enhancing Grid Security Through Public-Private Partnerships Act, will facilitate and encourage public-private partnerships in order to improve the cybersecurity of electric utilities.

Specifically, it would develop and provide for voluntary implementation of maturity models, self-assessments, and auditing methods for assessing the physical security and cybersecurity of electric utilities.

H.R. 2931 would provide training and technical assistance to electric utilities to address and mitigate cybersecurity supply chain management risks and increase opportunities for sharing best practices and data collection within the electric sector.

Finally, this legislation will require the Secretary of Energy to submit a report to Congress that assesses priorities, policies, procedures, actions, and implementations of electricity distribution systems to address threats to and vulnerabilities of such electricity distribution systems. We cannot allow criminal cyber behavior to go unchallenged. Both H.R. 2931 and H.R. 2928 will help in the fight against cyber attacks.

Mr. Speaker, I thank Chairman PALLONE, Chairman RUSH, leaders RODGERS and UPTON for their efforts to advance these bills, and I encourage all my colleagues to vote ''yes'' on final passage.

Mr. Speaker, 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), the Democratic sponsor.

Mr. MCNERNEY. Mr. Speaker, I thank the chairman for yielding.

Mr. Speaker, I rise today in support of my legislation, H.R. 2931, the Enhancing Grid Security Through Public-Private Partnership Act. The prior bill, this bill, and the next bill are good examples of working together on a bipartisan basis to accomplish things that are very critical to this country, and I thank my colleagues for being a very important part of this partnership.

Mr. Speaker, I am pleased that we are considering this bill today, because we simply can't afford to wait any longer to secure our Nation's critical infrastructure, including the grid. The Colonial Pipeline attack coming on the heels of the SolarWinds attack was a bright warning sign that we need to act quickly to pass this legislation.

Since the Colonial Pipeline attack, ransomware attacks have continued to skyrocket, and the need to enact H.R. 2931 has become even more pressing. H.R. 2931 would create a program to enhance the physical and cybersecurity of electric utilities. This program would develop methods for assessing security vulnerabilities. It would also provide cybersecurity training to electric utilities, advance cybersecurity of utility third-party vendors, and promote sharing of best practices and data collection in the electric sector.

Under this legislation, the Secretary of Energy would work in consultation with States, Federal agencies, and industry stakeholders to create this program. By encouraging these partnerships, we will better position ourselves to keep the Nation's lights on and to

protect our grid from the growing cyber threats.

Additionally, H.R. 2931 would require the Interruption Cost Estimate Calculator, which is used to calculate the ROI on utility investments, to be updated at least every 2 years to ensure accurate calculations.

Mr. Speaker, I thank my good friend and partner in this legislation, Representative LATTA from Ohio, for working with me on this important bill. I also thank Chairman PALLONE, Ranking Member RODGERS, and the staff of the committee for helping us move this legislation.

Mr. Speaker, I urge my colleagues to support it.

Mr. PALLONE. Mr. Speaker, I have no additional speakers, and I reserve the balance of my time.

Mr. LATTA. Mr. Speaker, again, from the recent attacks that we have had across the country in the last year and a half, it shows the importance of making sure that we are protected on the cybersecurity front. And working with my good friend and colleague from California, it has been so important that we get these two bills across the finish line today.

Mr. Speaker, I urge all Members today to support H.R. 2931, and I yield back the balance of my time.

Mr. PALLONE. Mr. Speaker, I would also ask that all our colleagues would support this on a bipartisan basis, 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. 2931.

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.

CYBER SENSE ACT OF 2021

Mr. PALLONE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 2928) 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.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 2928

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 2021''.

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 Ohio (Mr. LATTA) 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. 2928.

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. 2928, the Cyber Sense Act of 2021. Grid security is a national security issue. Fortunately, there has not yet been a broad cyberattack that has taken down large parts of the electric grid in the United States. But as we learned from the ransomware attack on the Colonial Pipeline earlier this year, we must not let our guard down.

Mr. Speaker, I am proud to support H.R. 2928, which gives the electric sector critical tools and technologies necessary to protect our grid from malicious harm.

This legislation gives the Department of Energy an important new authority to facilitate the adoption of more secure technologies and equipment in our Nation's grid. It does this by requiring the Department of Energy to set up a voluntary ''Cyber Sense'' program to identify cyber-secure products for use in the bulk-power system.

The bill also requires the Secretary of Energy 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.

□ 1430

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 want to again thank my colleagues, Representatives MCNERNEY and LATTA, for their hard work on this critical issue and for their persistence in pursuing this bill for the last several years. Their partnership and bipartisan leadership on cybersecurity issues continues to benefit us all.

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

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

Mr. Speaker, I rise today in support of H.R. 2928, the Cyber Sense Act, which is the second of two grid security bills that I have introduced and, again, worked closely on with my good friend and colleague, the gentleman from California (Mr. MCNERNEY).

This bipartisan legislation will establish a testing process under a newly established voluntary 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.

It would 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.

H.R. 2928 would also develop guidance for electric utilities for procurement of products and technologies and consider incentives to encourage the use of analysis and results of testing under the program in the design of products and technologies for use in the bulk-power system.

The SolarWinds attack exposed a vulnerability in our supply chains that