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

should serve as a wake-up call to the energy sector. Similar attacks on products used in grid operators' IT networks could go undetected and, when exposed, result in the costly process of disabling and removing such products from operation.

Having a program that would allow for the testing of a product's cybersecurity would help grid operators share information and maintain coordination with the Federal Government to keep pace with evolving cybersecurity threats. H.R. 2928 would accomplish these goals.

Again, I want to thank Chairman PALLONE, Chairman RUSH, Leader RODGERS, and Leader UPTON for their support. I call on my colleagues to support this bill, 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), the sponsor of the bill.

Mr. MCNERNEY. Mr. Speaker, I rise today in support of H.R. 2928, the Cyber Sense Act of 2021.

The Cyber Sense Act is another piece of bipartisan legislation that takes steps to improve the security of our Nation's electric grid infrastructure. It would establish a program to identify cyber secure products for the bulk-power grid through a testing and verification program.

The bulk-power system is essential for providing reliable electric power to the American people. We must ensure that this system is as secure as possible. Any vulnerable component in our grid is a threat to our security, and this bill will take important steps to strengthen the system.

It would also require the Department of Energy to provide technical assistance to electric utilities, manufacturers, and other relevant stakeholders related to cybersecurity vulnerabilities in products under the Cyber Sense program.

In today's world, there are literally billions of connected devices in use and the number is rapidly increasing. Most of these devices have no standards. There is no way for electric utilities to verify the security of the products, and we are seeing cyber threats continue to increase. This legislation is badly needed.

Mr. Speaker, I thank my good friend, Mr. LATTA, again for his partnership on this bill. We have been working together on a number of issues, and this is a sign of our partnership.

I also thank Chairman PALLONE and Ranking Member RODGERS for working with us to move this legislation quickly, and I don't want to forget the staff of the Energy and Commerce Committee, who have been so helpful.

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

Mr. LATTA. Mr. Speaker, I have no other speakers, and I am ready to close.

Mr. Speaker, again, as the gentleman from California mentioned about the ongoing cyberattacks we have had in this country, it is absolutely essential that we get this bill across the finish line. H.R. 2928 is going to help accomplish these goals and protect our grid out there.

Mr. Speaker, I urge all of my colleagues to support this legislation, and I yield back the balance of my time.

Mr. PALLONE. Mr. Speaker, I urge my colleagues on both sides to support 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 New Jersey (Mr. PALLONE) that the House suspend the rules and pass the bill, H.R. 2928.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. ROSENDALE. Mr. Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3(s) of House Resolution 8, the yeas and nays are ordered.

Pursuant to clause 8 of rule XX, further proceedings on this motion are postponed.

EMERGENCY REPORTING ACT

Mr. PALLONE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 1250) to direct the Federal Communications Commission to issue reports after activation of the Disaster Information Reporting System and to make improvements to network outage reporting.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 1250

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 ''Emergency Reporting Act''.

SEC. 2. REPORTS AFTER ACTIVATION OF DISASTER INFORMATION REPORTING SYSTEM; IMPROVEMENTS TO NETWORK OUTAGE REPORTING.

(a) REPORTS AFTER ACTIVATION OF DISASTER INFORMATION REPORTING SYSTEM.—

(1) PRELIMINARY REPORT.—

(A) IN GENERAL.—Not later than 6 weeks after the deactivation of the Disaster Information Reporting System with respect to an event for which the System was activated for at least 7 days, the Commission shall issue a preliminary report on, with respect to such event and to the extent known—

(i) the number and duration of any outages of—

(I) broadband internet access service;

(II) interconnected VoIP service;

(III) commercial mobile service; and

(IV) commercial mobile data service;

(ii) the approximate number of users or the amount of communications infrastructure potentially affected by an outage described in clause (i);

(iii) the number and duration of any outages at public safety answering points that prevent public safety answering points from receiving emergency calls and routing such calls to emergency service personnel; and

(iv) any additional information determined appropriate by the Commission.

(B) DEVELOPMENT OF REPORT.—The Commission shall develop the report required by subparagraph (A) using information collected by the Commission, including information collected by the Commission through the System.

(2) PUBLIC FIELD HEARINGS.—

(A) REQUIREMENT.—Not later than 8 months after the deactivation of the Disaster Information Reporting System with respect to an event for which the System was activated for at least 7 days, the Commission shall hold at least 1 public field hearing in the area affected by such event.

(B) INCLUSION OF CERTAIN INDIVIDUALS IN HEARINGS.—For each public field hearing held under subparagraph (A), the Commission shall consider including—

(i) representatives of State government, local government, or Indian Tribal governments in areas affected by such event;

(ii) residents of the areas affected by such event, or consumer advocates;

(iii) providers of communications services affected by such event;

(iv) faculty of institutions of higher education;

(v) representatives of other Federal agencies;

(vi) electric utility providers;

(vii) communications infrastructure companies; and

(viii) first responders, emergency managers, or 9–1–1 directors in areas affected by such event.

(3) FINAL REPORT.—Not later than 12 months after the deactivation of the Disaster Information Reporting System with respect to an event for which the System was activated for at least 7 days, the Commission shall issue a final report that includes, with respect to such event—

(A) the information described under paragraph (1)(A); and

(B) any recommendations of the Commission on how to improve the resiliency of affected communications or networks recovery efforts.

(4) DEVELOPMENT OF REPORTS.—In developing a report required under this subsection, the Commission shall consider information collected by the Commission, including information collected by the Commission through the System, and any public hearing described in paragraph (2) with respect to the applicable event.

(5) PUBLICATION.—The Commission shall publish each report, excluding information that is otherwise exempt from public disclosure under the rules of the Commission, issued under this subsection on the website of the Commission upon the issuance of such report.

(b) IMPROVEMENTS TO NETWORK OUTAGE REPORTING.—Not later than 1 year after the date of the enactment of this Act, the Commission shall conduct a proceeding and, after public notice and an opportunity for comment, adopt rules to—

(1) determine the circumstances under which to require service providers subject to the 9–1–1 regulations established under part 9 of title 47, Code of Federal Regulations, to submit a timely notification, (in an easily accessible format that facilities situational awareness) to public safety answering points regarding communications service disruptions within the assigned territories of such public safety answering points that prevent—

(A) the origination of 9–1–1 calls;

(B) the delivery of Automatic Location Information; or

(C) Automatic Number Identification;

(2) require such notifications to be made; and

(3) specify the appropriate timing of such notification.