and 70 percent of physicians believe additional training in rare diseases would be helpful.

A rare disease can spread and worsen during the lengthy time before diagnosis and the start of the proper treatment.

I ask my colleagues to join me in supporting this bill.

Ms. ESHOO. Madam Speaker, I rise in support of H.R. 4439, the Creating Hope Reauthorization Act. I'm proud to have advanced this bipartisan bill through my Health Subcommittee and I'm pleased to support it on the Floor today.

The Creating Hope Reauthorization Act sponsored by Representative G.K. BUTTERFIELD helps children access pediatric cancer drugs.

Pediatric cancer is the number one disease killer of American children, but pharmaceutical companies often avoid developing pediatric cancer drugs because of the small market and the high risks associated with studying and testing drugs for children.

The Creating Hope Reauthorization Act provides incentives for the research and development of pediatric cancer drugs by providing the developers with the valuable Priority Review Vouchers which allow the recipient to speed up the FDA review of any one of its new drug products.

Since its passage the GAO studied the pediatric priority review vouchers and found that pharmaceutical developers said Priority Review Vouchers were a factor in drug development decisions.

Dr. Crystal Mackall of the Stanford Center for Cancer Cell Therapy said that, ''The voucher program has been remarkedly impactful for childhood cancers. Before the program, I used to go with my hat in hand to beg investors to consider a potential drug. Now people take a second look and are interested in developing drugs. We're just getting started on this new way of thinking about children's drugs. The voucher program required a culture change around how to think of the pediatric drug business model, which in the drug development world could take a while.''

As Dr. Mackall said, this program seeks to shift decision-making early in the lengthy drug development cycle. A lengthy reauthorization of 4 years as offered in the AINS will be beneficial for this decision-making and I urge my colleagues to support this bill.

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. 4439, as amended.

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

The title of the bill was amended so as to read: ''A bill to amend the Federal Food, Drug, and Cosmetic Act to extend the authority of the Secretary of Health and Human Services to issue priority review vouchers to encourage treatments for rare pediatric diseases.''.

A motion to reconsider was laid on the table.

□ 1645

GRID SECURITY RESEARCH AND DEVELOPMENT ACT

Mr. BERA. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 5760) to provide for a comprehensive interdisciplinary research, development, and demonstration initiative to strengthen the capacity of the energy sector to prepare for and withstand cyber and physical attacks, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5760

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 ''Grid Security Research and Development Act''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) The Nation, and every critical infrastructure sector, depends on reliable electricity.

(2) Intelligent electronic devices, advanced analytics, and information systems used across the energy sector are essential to maintaining reliable operation of the electric grid.

(3) The cybersecurity threat landscape is constantly changing and attacker capabilities are advancing rapidly, requiring ongoing modifications, advancements, and investments in technologies and procedures to maintain security.

(4) It is in the national interest for Federal agencies to invest in cybersecurity research that informs and facilitates private sector investment and use of advanced cybersecurity tools and procedures to protect information systems.

(5) The number of devices and systems connecting to the electric grid is increasing, and integrating cybersecurity protections into information systems when they are built is more effective than modifying products after installation to meet cybersecurity goals.

(6) An understanding of human factors can be leveraged to understand the behavior of cyber threat actors, develop strategies to counter threat actors, improve cybersecurity training programs, optimize the design of human-machine interfaces and cybersecurity tools, and increase the capacity of the energy sector workforce to prevent unauthorized access to critical systems.

SEC. 3. AMENDMENT TO ENERGY INDEPENDENCE AND SECURITY ACT OF 2007.

Title XIII of the Energy Independence and Security Act of 2007 (42 U.S.C. 17381 et seq.) is amended by adding at the end the following:

''SEC. 1310. ENERGY SECTOR SECURITY RESEARCH, DEVELOPMENT, AND DEMONSTRATION PROGRAM.

''(a) IN GENERAL.—The Secretary, in coordination with appropriate Federal agencies, the Electricity Subsector Coordinating Council, the Electric Reliability Organization, State, tribal, local, and territorial governments, the private sector, and other relevant stakeholders, shall carry out a research, development, and demonstration program to protect the electric grid and energy systems, including assets connected to the distribution grid, from cyber and physical attacks by increasing the cyber and physical security capabilities of the energy sector and accelerating the development of relevant technologies and tools.

''(b) DEPARTMENT OF ENERGY.—As part of the initiative described in subsection (a), the Secretary shall award research, development, and demonstration grants to—

''(1) identify cybersecurity risks to information systems within, and impacting, the electricity sector, energy systems, and energy infrastructure;

''(2) develop methods and tools to rapidly detect cyber intrusions and cyber incidents, including through the use of data and big data analytics techniques, such as intrusion detection, and security information and event management systems, to validate and verify system behavior;

''(3) assess emerging cybersecurity capabilities that could be applied to energy systems and develop technologies that integrate cybersecurity features and procedures into the design and development of existing and emerging grid technologies, including renewable energy, storage, and demand-side management technologies;

''(4) identify existing vulnerabilities in intelligent electronic devices, advanced analytics systems, and information systems;

''(5) work with relevant entities to develop technologies or concepts that build or retrofit cybersecurity features and procedures into—

''(A) information and energy management system devices, components, software, firmware, and hardware, including distributed control and management systems, and building management systems;

''(B) data storage systems, data management systems, and data analysis processes;

''(C) automated- and manually-controlled devices and equipment for monitoring and stabilizing the electric grid;

''(D) technologies used to synchronize time and develop guidance for operational contingency plans when time synchronization technologies, are compromised;

''(E) power system delivery and end user systems and devices that connect to the grid, including—

''(i) meters, phasor measurement units, and other sensors;

''(ii) distribution automation technologies, smart inverters, and other grid control technologies;

''(iii) distributed generation, energy storage, and other distributed energy technologies;

''(iv) demand response technologies;

''(v) home and building energy management and control systems;

''(vi) electric and plug-in hybrid vehicles and electric vehicle charging systems; and

''(vii) other relevant devices, software, firmware, and hardware; and

''(F) the supply chain of electric grid management system components;

''(6) develop technologies that improve the physical security of information systems, including remote assets;

''(7) integrate human factors research into the design and development of advanced tools and processes for dynamic monitoring, detection, protection, mitigation, response, and cyber situational awareness;

''(8) evaluate and understand the potential consequences of practices used to maintain the cybersecurity of information systems and intelligent electronic devices;

''(9) develop or expand the capabilities of existing cybersecurity test beds to simulate impacts of cyber attacks and combined cyber-physical attacks on information systems and electronic devices, including by increasing access to existing and emerging test beds for cooperative utilities, utilities owned by a political subdivision of a State, such as municipally-owned electric utilities, and other relevant stakeholders; and

''(10) develop technologies that reduce the cost of implementing effective cybersecurity technologies and tools, including updates to these technologies and tools, in the energy sector.

''(c) NATIONAL SCIENCE FOUNDATION.—The National Science Foundation, in coordination with other Federal agencies as appropriate, shall through its cybersecurity research and development programs—

''(1) support basic research to advance knowledge, applications, technologies, and tools to strengthen the cybersecurity of information systems, including electric grid and energy systems, including interdisciplinary research in—

''(A) evolutionary systems, theories, mathematics, and models;

''(B) economic and financial theories, mathematics, and models; and

''(C) big data analytical methods, mathematics, computer coding, and algorithms; and

''(2) support cybersecurity education and training focused on information systems for the electric grid and energy workforce, including through the Advanced Technological Education program, the Cybercorps program, graduate research fellowships, and other appropriate programs.

''(d) DEPARTMENT OF HOMELAND SECURITY SCIENCE AND TECHNOLOGY DIRECTORATE.—The Science and Technology Directorate of the Department of Homeland Security shall coordinate with the Department of Energy, the private sector, and other relevant stakeholders, to research existing cybersecurity technologies and tools used in the defense industry in order to—

''(1) identify technologies and tools that may meet civilian energy sector cybersecurity needs;

''(2) develop a research strategy that incorporates human factors research findings to guide the modification of defense industry cybersecurity tools for use in the civilian sector;

''(3) develop a strategy to accelerate efforts to bring modified defense industry cybersecurity tools to the civilian market; and

''(4) carry out other activities the Secretary of Homeland Security considers appropriate to meet the goals of this subsection.

''SEC. 1311. GRID RESILIENCE AND EMERGENCY RESPONSE.

''(a) IN GENERAL.—Not later than 180 days after the enactment of the Grid Security Research and Development Act, the Secretary shall establish a research, development, and demonstration program to enhance resilience and strengthen emergency response and management pertaining to the energy sector.

''(b) GRANTS.—The Secretary shall award grants to eligible entities under subsection (c) on a competitive basis to conduct research and development with the purpose of improving the resilience and reliability of electric grid by—

''(1) developing methods to improve community and governmental preparation for and emergency response to large-area, long-duration electricity interruptions, including through the use of energy efficiency, storage, and distributed generation technologies;

''(2) developing tools to help utilities and communities ensure the continuous delivery of electricity to critical facilities;

''(3) developing tools to improve coordination between utilities and relevant Federal agencies to enable communication, information-sharing, and situational awareness in the event of a physical or cyber-attack on the electric grid;

''(4) developing technologies and capabilities to withstand and address the current and projected impact of the changing climate on energy sector infrastructure, including extreme weather events and other natural disasters;

''(5) developing technologies capable of early detection of malfunctioning electrical equipment on the transmission and distribution grid, including detection of spark ignition causing wildfires and risks of vegetation contact;

''(6) assessing upgrades and additions needed to energy sector infrastructure due to projected changes in the energy generation mix and energy demand; and

''(7) upgrading tools used to estimate the costs of outages longer than 24 hours.

''(8) developing tools and technologies to assist with the planning, safe execution of, and safe and timely restoration of power after emergency power shut offs, such as those conducted to reduce risks of wildfires started by grid infrastructure.

''(c) ELIGIBLE ENTITIES.—The entities eligible to receive grants under this section include—

''(1) an institution of higher education;

''(2) a nonprofit organization;

''(3) a National Laboratory;

''(4) a unit of State, local, or tribal government;

''(5) an electric utility or electric cooperative;

''(6) a retail service provider of electricity;

''(7) a private commercial entity;

''(8) a partnership or consortium of 2 or more entities described in subparagraphs (1) through (7); and

''(9) any other entities the Secretary deems appropriate.

''(d) RELEVANT ACTIVITIES.—Grants awarded under subsection (b) shall include funding for research and development activities related to the purpose described in subsection (b), such as—

''(1) development of technologies to use distributed energy resources, such as solar photovoltaics, energy storage systems, electric vehicles, and microgrids, to improve grid and critical end-user resilience;

''(2) analysis of non-technical barriers to greater integration and use of technologies on the distribution grid;

''(3) analysis of past large-area, long-duration electricity interruptions to identify common elements and best practices for electricity restoration, mitigation, and prevention of future disruptions;

''(4) development of advanced monitoring, analytics, operation, and controls of electric grid systems to improve electric grid resilience;

''(5) analysis of technologies, methods, and concepts that can improve community resilience and survivability of frequent or long-duration power outages;

''(6) development of methodologies to maintain cybersecurity during restoration of energy sector infrastructure and operation;

''(7) development of advanced power flow control systems and components to improve electric grid resilience; and

''(8) any other relevant activities determined by the Secretary.

''(e) TECHNICAL ASSISTANCE.—

''(1) IN GENERAL.—The Secretary shall provide technical assistance to eligible entities for the commercial application of technologies to improve the resilience of the electric grid and commercial application of technologies to help entities develop plans for preventing and recovering from various power outage scenarios at the local, regional, and State level.

''(2) TECHNICAL ASSISTANCE PROGRAM.—The commercial application technical assistance program established in paragraph (1) shall include assistance to eligible entities for—

''(A) the commercial application of technologies developed from the grant program established in subsection (b), including cooperative utilities and utilities owned by a political subdivision of a State, such as municipally-owned electric utilities;

''(B) the development of methods to strengthen or otherwise mitigate adverse impacts on electric grid infrastructure against natural hazards;

''(C) the use of Department data and modeling tools for various purposes;

''(D) a resource assessment and analysis of future demand and distribution requirements, including development of advanced grid architectures and risk analysis; and

''(E) the development of tools and technologies to coordinate data across relevant entities to promote resilience and wildfire prevention in the planning, design, construction, operation, and maintenance of transmission infrastructure;

''(F) analysis to predict the likelihood of extreme weather events to inform the planning, design, construction, operation, and maintenance of transmission infrastructure in consultation with the National Oceanic and Atmospheric Administration; and

''(G) the commercial application of relevant technologies, such as distributed energy resources, microgrids, or other energy technologies, to establish backup power for users or facilities affected by emergency power shutoffs.

''(3) ELIGIBLE ENTITIES.—The entities eligible to receive technical assistance for commercial application of technologies under this section include—

''(A) representatives of all sectors of the electric power industry, including electric utilities, trade organizations, and transmission and distribution system organizations, owners, and operators;

''(B) State and local governments and regulatory authorities, including public utility commissions;

''(C) tribal and Alaska Native governmental entities;

''(D) partnerships among entities under subparagraphs (A) through (C);

''(E) regional partnerships; and

''(F) any other entities the Secretary deems appropriate.

''(4) AUTHORITY.—Nothing in this section shall authorize the Secretary to require any entity to adopt any model, tool, technology, plan, analysis, or assessment.

''SEC. 1312. BEST PRACTICES AND GUIDANCE DOCUMENTS FOR ENERGY SECTOR CYBERSECURITY RESEARCH.

''(a) IN GENERAL.—The Secretary, in coordination with appropriate Federal agencies, the Electricity Subsector Coordinating Council, standards development organizations, State, tribal, local, and territorial governments, the private sector, public utility commissions, and other relevant stakeholders, shall coordinate the development of guidance documents for research, development, and demonstration activities to improve the cybersecurity capabilities of the energy sector through participating agencies. As part of these activities, the Secretary shall—

''(1) facilitate stakeholder involvement to update—

''(A) the Roadmap to Achieve Energy Delivery Systems Cybersecurity;

''(B) the Cybersecurity Procurement Language for Energy Delivery Systems, including developing guidance for—

''(i) contracting with third parties to conduct vulnerability testing for information systems used across the energy production, delivery, storage, and end use systems;

''(ii) contracting with third parties that utilize transient devices to access information systems; and

''(iii) managing supply chain risks; and

''(C) the Electricity Subsector Cybersecurity Capability Maturity Model, including the development of metrics to measure changes in cybersecurity readiness; and

''(2) develop voluntary guidance to improve digital forensic analysis capabilities, including—

''(A) developing standardized terminology and monitoring processes; and

''(B) utilizing human factors research to develop more effective procedures for logging incident events; and

''(3) work with the National Science Foundation, Department of Homeland Security, and stakeholders to develop a mechanism to anonymize, aggregate, and share the testing results from cybersecurity test beds to facilitate technology improvements by public and private sector researchers.

''(b) BEST PRACTICES.—The Secretary, in collaboration with the Director of the National Institute of Standards and Technology and other appropriate Federal agencies, shall convene relevant stakeholders and facilitate the development of—

''(1) consensus-based best practices to improve cybersecurity for—

''(A) emerging energy technologies;

''(B) distributed generation and storage technologies, and other distributed energy resources;

''(C) electric vehicles and electric vehicle charging stations; and

''(D) other technologies and devices that connect to the electric grid;

''(2) recommended cybersecurity designs and technical requirements that can be used by the private sector to design and build interoperable cybersecurity features into technologies that connect to the electric grid, including networked devices and components on distribution systems; and

''(3) technical analysis that can be used by the private sector in developing best practices for test beds and test bed methodologies that will enable reproducible testing of cybersecurity protections for information systems, electronic devices, and other relevant components, software, and hardware across test beds.

''(c) REGULATORY AUTHORITY.—None of the activities authorized in this section shall be construed to authorize regulatory actions. Additionally, the voluntary standards developed under this section shall not duplicate or conflict with mandatory reliability standards.

''SEC. 1313. VULNERABILITY TESTING AND TECHNICAL ASSISTANCE TO IMPROVE CYBERSECURITY.

''(a) IN GENERAL.—The Secretary shall—

''(1) coordinate with energy sector asset owners and operators, leveraging the research facilities and expertise of the National Laboratories, to assist entities in developing testing capabilities by—

''(A) utilizing a range of methods to identify vulnerabilities in physical and cyber systems;

''(B) developing cybersecurity risk assessment tools and providing analyses and recommendations to participating stakeholders; and

''(C) working with stakeholders to develop methods to share anonymized and aggregated test results to assist relevant stakeholders in the energy sector, researchers, and the private sector to advance cybersecurity efforts, technologies, and tools;

''(2) collaborate with relevant stakeholders, including public utility commissions, to—

''(A) identify information, research, staff training, and analytical tools needed to evaluate cybersecurity issues and challenges in the energy sector; and

''(B) facilitate the sharing of information and the development of tools identified under subparagraph (A);

''(3) collaborate with tribal governments to identify information, research, and analysis tools needed by tribal governments to increase the cybersecurity of energy assets within their jurisdiction.

''SEC. 1314. EDUCATION AND WORKFORCE TRAINING RESEARCH AND STANDARDS.

''(a) IN GENERAL.—The Secretary shall support the development of a cybersecurity workforce through a program that—

''(1) facilitates collaboration between undergraduate and graduate students, researchers at the National Laboratories, and the private sector;

''(2) prioritizes science and technology in areas relevant to the mission of the Department of Energy through the design and application of cybersecurity technologies;

''(3) develops, or facilitates private sector development of, voluntary cybersecurity training and retraining standards, lessons, and recommendations for the energy sector that minimize duplication of cybersecurity compliance training programs; and

''(4) maintains a public database of cybersecurity education, training, and certification programs.

''(b) GRID RESILIENCE TECHNOLOGY TRAINING.—The Secretary shall support the development of the grid workforce through a training program that prioritizes activities that enhance the resilience of the electric grid and energy sector infrastructure, including training on the use of tools, technologies, and methods developed under the grant program established in section 1311(b).

''(c) COLLABORATION.—In carrying out the program authorized in subsection (a) and (b), the Secretary shall leverage programs and activities carried out across the Department of Energy, other relevant Federal agencies, institutions of higher education, and other appropriate entities best suited to provide national leadership on cybersecurity and grid resilience-related issues.

''SEC. 1315. INTERAGENCY COORDINATION AND STRATEGIC PLAN FOR ENERGY SECTOR CYBERSECURITY RESEARCH.

''(a) DUTIES.—The Secretary, in coordination with the Energy Sector Government Coordinating Council, shall—

''(1) review the most recent versions of the Roadmap to Achieve Energy Delivery Systems Cybersecurity and the Multi-Year Program Plan for Energy Sector Cybersecurity to identify crosscutting energy sector cybersecurity research needs and opportunities for collaboration among Federal agencies and other relevant stakeholders;

''(2) identify interdisciplinary research, technology, and tools that can be applied to cybersecurity challenges in the energy sector;

''(3) identify technology transfer opportunities to accelerate the development and commercial application of novel cybersecurity technologies, systems, and processes in the energy sector; and

''(4) develop a coordinated Interagency Strategic Plan for research to advance cybersecurity capabilities used in the energy sector that builds on the Roadmap to Achieve Energy Delivery Systems in Cybersecurity and the Multi-Year Program Plan for Energy Sector Cybersecurity.

''(b) INTERAGENCY STRATEGIC PLAN.—

''(1) SUBMITTAL.—The Interagency Strategic Plan developed under subsection (a)(4) shall be submitted to Congress and made public within 12 months after the date of enactment of the Grid Security Research and Development Act.

''(2) CONTENTS.—The Interagency Strategic Plan shall include—

''(A) an analysis of how existing cybersecurity research efforts across the Federal Government are advancing the goals of the Roadmap to Achieve Energy Delivery Systems Cybersecurity and the Multi-Year Program Plan for Energy Sector Cybersecurity;

''(B) recommendations for research areas that may advance the cybersecurity of the energy sector;

''(C) an overview of existing and proposed public and private sector research efforts that address the topics outlined in paragraph (3); and

''(D) an overview of needed support for workforce training in cybersecurity for the energy sector.

''(3) CONSIDERATIONS.—In developing the Interagency Strategic Plan, the Secretary, in coordination with the Energy Sector Government Coordinating Council, shall consider—

''(A) opportunities for human factors research to improve the design and effectiveness of cybersecurity devices, technologies, tools, processes, and training programs;

''(B) contributions of other disciplines to the development of innovative cybersecurity procedures, devices, components, technologies, and tools;

''(C) opportunities for technology transfer programs to facilitate private sector development of cybersecurity procedures, devices, components, technologies, and tools for the energy sector;

''(D) broader applications of the work done by relevant Federal agencies to advance the cybersecurity of information systems and data analytics systems for the energy sector; and

''(E) activities called for in the Federal cybersecurity research and development strategic plan required by section 201(a)(1) of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7431(a)(1)).

''(c) PARTICIPATION.—For the purposes of carrying out this section, the Energy Sector Government Coordinating Council shall include representatives from Federal agencies with expertise in the energy sector, information systems, data analytics, cyber and physical systems, engineering, human factors research, human-machine interfaces, high performance computing, big data and data analytics, or other disciplines considered appropriate by the Council Chair.

''SEC. 1316. REPORT TO CONGRESS.

''(a) BALANCING RISKS, INCREASING SECURITY, AND IMPROVING MODERNIZATION.—

''(1) STUDY.—The Secretary, in collaboration with the National Institute of Standards and Technology, other Federal agencies, and energy sector stakeholders, in order to provide recommendations for additional research, development, demonstration, and commercial application activities, shall—

''(A) analyze physical and cyber attacks on energy sector infrastructure and information systems and identify cost-effective opportunities to improve physical and cyber security; and

''(B) examine the risks associated with increasing penetration of digital technologies in grid networks, particularly on the distribution grid.

''(2) CONTENT.—The study shall—

''(A) analyze processes, operational procedures, and other factors common among cyber attacks;

''(B) identify areas where human behavior plays a critical role in maintaining or compromising the security of a system;

''(C) recommend—

''(i) changes to the design of devices, human-machine interfaces, technologies, tools, processes, or procedures to optimize security that do not require a change in human behavior; and

''(ii) training techniques to increase the capacity of employees to actively identify, prevent, or neutralize the impact of cyber attacks;

''(D) evaluate existing engineering and technical design criteria and guidelines that incorporate human factors research findings, and recommend criteria and guidelines for cybersecurity tools that can be used to develop display systems for cybersecurity monitoring, such as alarms, user-friendly displays, and layouts;

''(E) evaluate the cybersecurity risks and benefits of various design and architecture options for energy sector systems, networked grid systems and components, and automation systems, including consideration of—

''(i) designs that include both digital and analog control devices and technologies;

''(ii) different communication technologies used to transfer information and data between control system devices, technologies, and system operators;

''(iii) automated and human-in-the-loop devices and technologies;

''(iv) programmable versus nonprogrammable devices and technologies;

''(v) increased redundancy using dissimilar cybersecurity technologies; and

''(vi) grid architectures that use autonomous functions to limit control vulnerabilities; and

''(F) recommend methods or metrics to document changes in risks associated with system designs and architectures.

''(3) CONSULTATION.—In conducting the study, the Secretary shall consult with energy sector stakeholders, academic researchers, the private sector, and other relevant stakeholders.

''(4) REPORT.—Not later than 24 months after the date of enactment of the Grid Security Research and Development Act, the Secretary shall submit the study to the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Energy and Natural Resources of the Senate.

''SEC. 1317. DEFINITIONS.

''In this title:

''(1) BIG DATA.—The term 'big data' means datasets that require advanced analytical methods for their transformation into useful information.

''(2) CYBERSECURITY.—The term 'cybersecurity' means protecting an information system or

information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

''(3) CYBERSECURITY THREAT.—The term 'cybersecurity threat' has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

''(4) ELECTRICITY SUBSECTOR COORDINATING COUNCIL.—The term 'Electricity Subsector Coordinating Council' means the self-organized, self-governed council consisting of senior industry representatives to serve as the principal liaison between the Federal Government and the electric power sector and to carry out the role of the Sector Coordinating Council as established in the National Infrastructure Protection Plan for the electricity subsector.

''(5) ENERGY SECTOR GOVERNMENT COORDINATING COUNCIL.—The term 'Energy Sector Government Coordinating Council' means the council consisting of representatives from relevant Federal Government agencies to provide effective coordination of energy sector efforts to ensure a secure, reliable, and resilient energy infrastructure and to carry out the role of the Government Coordinating Council as established in the National Infrastructure Protection Plan for the energy sector.

''(6) HUMAN FACTORS RESEARCH.—The term 'human factors research' means research on human performance in social and physical environments, and on the integration and interaction of humans with physical systems and computer hardware and software.

''(7) HUMAN-MACHINE INTERFACES.—The term 'human-machine interfaces' means technologies that present information to an operator or user about the state of a process or system, or accept human instructions to implement an action, including visualization displays such as a graphical user interface.

''(8) INFORMATION SYSTEM.—The term 'information system'—

''(A) has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501); and

''(B) includes operational technology, information technology, and communications.

''(9) NATIONAL LABORATORY.—The term 'national laboratory' has the meaning given the term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

''(10) SECURITY VULNERABILITY.—The term 'security vulnerability' has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

''(11) TRANSIENT DEVICES.—The term 'transient devices' means removable media, including floppy disks, compact disks, USB flash drives, external hard drives, mobile devices, and other devices that utilize wireless connections.

''SEC. 1318. AUTHORIZATION OF APPROPRIATIONS.

''There are authorized to be appropriated to the Secretary to carry out this Act—

''(1) $150,000,000 for fiscal year 2021;

''(2) $157,500,000 for fiscal year 2022;

''(3) $165,375,000 for fiscal year 2023;

''(4) $173,645,000 for fiscal year 2024; and

''(5) $182,325,000 for fiscal year 2025.''.

SEC. 4. CRITICAL INFRASTRUCTURE RESEARCH AND CONSTRUCTION.

(a) IN GENERAL.—The Secretary shall carry out a program of research, development, and demonstration of technologies and tools to help ensure the resilience and security of critical integrated grid infrastructures.

(b) CRITICAL INFRASTRUCTURE DEFINED.—The term ''critical infrastructure'' means infrastructure that the Secretary determines to be vital to socioeconomic activities such that, if destroyed or damaged, such destruction or damage could cause substantial disruption to such socioeconomic activities.

(c) COORDINATION.—In carrying out the program under subsection (a), the Secretary shall leverage expertise and resources of and facilitate collaboration and coordination between—

(1) relevant programs and activities across the Department;

(2) the Department of Defense; and

(3) the Department of Homeland Security.

(d) CRITICAL INFRASTRUCTURE TEST FACILITY.—In carrying out the program under subsection (a), the Secretary shall establish and operate a Critical Infrastructure Test Facility (referred to in this section as the ''Test Facility'') that allows for scalable physical and cyber performance testing to be conducted on industry-scale critical infrastructure systems. This facility shall include a focus on—

(1) cybersecurity test beds; and

(2) electric grid test beds.

(e) SELECTION.—The Secretary shall select the Test Facility under this section on a competitive, merit-reviewed basis. The Secretary shall consider applications from National Laboratories, institutions of higher education, multi-institutional collaborations, and other appropriate entities.

(f) DURATION.—The Test Facility established under this section shall receive support for a period of not more than 5 years, subject to the availability of appropriations.

(g) RENEWAL.—Upon the expiration of any period of support of the Test Facility, the Secretary may renew support for the Test Facility, on a merit-reviewed basis, for a period of not more than 5 years.

(h) TERMINATION.—Consistent with the existing authorities of the Department, the Secretary may terminate the Test Facility for cause during the performance period.

SEC. 5. CONFORMING AMENDMENT.

Section 1(b) of the Energy Independence and Security Act of 2007 is amended in the table of contents by adding after the matter relating to section 1309 the following:

''Sec. 1310. Energy sector security research, development, and demonstration program.

''Sec. 1311. Grid resilience and emergency response.

''Sec. 1312. Best practices and guidance documents for energy sector cybersecurity research.

''Sec. 1313. Vulnerability testing and technical assistance to improve cybersecurity.

''Sec. 1314. Education and workforce training research and standards.

''Sec. 1315. Interagency coordination and strategic plan for energy sector cybersecurity research.

''Sec. 1316. Report to Congress.

''Sec. 1317. Definitions.

''Sec. 1318. Authorization of appropriations.''.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from California (Mr. BERA) and the gentleman from Oklahoma (Mr. LUCAS) each will control 20 minutes.

The Chair recognizes the gentleman from California.

GENERAL LEAVE

Mr. BERA. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and to include extraneous material on H.R. 5760, the bill now under consideration.

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

There was no objection.

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

Mr. Speaker, I rise today in support of my bill, H.R. 5760, the Grid Security Research and Development Act.

I first want to thank the chairwoman of the Committee on Science, Space, and Technology, Ms. JOHNSON, and the ranking member, Mr. LUCAS, for their help in passing the Grid Security R&D bill out of the Committee on Science, Space, and Technology and bringing it to the floor.

I also thank my colleague, Congressman RANDY WEBER from Texas, for joining on as a bipartisan cosponsor.

Mr. Speaker, the Grid Security R&D Act supports sustained investment across Federal agencies in research and technology to keep pace with the rapidly evolving threats to our electrical grid. The bill focuses on protecting our grid from two major threats: Cyber and physical.

Access to reliable power is core to our economy, and the impact of physical threats to our electric grid have never been clearer than now.

This summer, in my home State of California, the scenario of high winds, combined with lightning strikes and dry ground, have created some of the most dangerous wildfires in our State's history. In addition to burning millions of acres and causing loss of life, these wildfires put a significant part of our region on notice for potential emergency power shutoffs to reduce the risk of new outbreaks and further wildfire damage.

However, these shutoffs are not as simple as turning off and on a light switch. It takes time to de-energize transmission systems in advance of a severe weather event and to reenergize the system after the threat has passed.

While safety and preventing wildfires is a high priority, these shutoffs can leave hundreds of thousands of people without power for a few days. Dangerous wildfires, intense periods of drought, and other severe weather events have become increasingly more common in recent years because of climate change and will continue to threaten our grid.

Furthermore, the inability to protect our grid from these severe weather events becomes more magnified during significant emergencies like the COVID–19 pandemic.

Our hospitals and emergency rooms are working around the clock to save lives. They need access to reliable power and the assurance to know that the power will not go out during an important surgery or stop a ventilator from running.

In addition, food banks and restaurants rely on refrigeration to continue supplying food to those in need and our small businesses cannot reopen if they can't keep the lights on.

Ensuring access to electricity is critical in times like this. That is why I am proud to lead this bill, which would help strengthen the resiliency of our electric grid against physical threats. Our bill would also provide funding to develop technologies that would toughen our grid against wildfires and other natural disasters by improving early detection of deteriorating electrical transmission and distribution systems.

This aging equipment can tend to spark and come in contact with vegetation during high-wind events and natural disasters causing wildfires.

This bill will also spur the development and implementation of microgrid and battery storage technologies, provide backup power options so that in the event of an emergency power shutoff, a more targeted shutoff will impact less households.

The threat of climate change in our electric grid is real. We have an opportunity to continue the modernization of our power system infrastructure, and this bill is a step in the right direction.

Mr. Speaker, the other focus of our bill is improving cybersecurity across our electric grid. As the grid and other forms of critical infrastructure become more digitized, the risk that cyberattacks would shut down critical systems has increased, and in some cases these attacks can even cause physical damage to the grid. The types of cyberattacks also continue to become more sophisticated.

Last year, cyber hackers remotely attacked electric grid networks for the first time, affecting several Western States, including California, Utah, and Wyoming. Given how critical reliable access to power is to our daily lives, these attacks highlight the need for investment to address this evolving threat.

H.R. 5760 would authorize a comprehensive, coordinated research effort across Federal agencies to advance cybersecurity capabilities for the energy sector.

Research areas would include: improving rapid detection of cyber intrusions, integrating cybersecurity features into the energy infrastructure, and focusing in on cyber solutions through our defense sector that can be modified and transferred to the civilian power sector.

Lastly, our bill invests in strengthening our cybersecurity workforce. As our electric grid continues to modernize with renewable energy and energy storage technologies, a high-skilled workforce will be needed who understand the evolving threats.

I look forward to working with the Senate to get this bill passed into law so we can continue to improve the resiliency of our electric grid.

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

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC, September 2, 2020.

Hon. EDDIE BERNICE JOHNSON,
Chairwoman, Committee on Science, Space and Technology, House of Representatives, Washington, DC.

DEAR CHAIRWOMAN JOHNSON: I write to you regarding H.R. 5760, the ''Grid Security Research and Development Act.''

H.R. 5760 contains provisions that fall within the jurisdiction of the Committee on Homeland Security. I recognize and appreciate your desire to see this legislation implemented and accordingly, I will not seek a sequential referral of the bill. However, agreeing to waive consideration of this bill should not be construed as the Committee on Homeland Security waiving, altering, or otherwise affecting its jurisdiction over subject matters contained in the bill which fall within its Rule X jurisdiction.

I would also ask that a copy of this letter and your response be included in the legislative report on H.R. 5760 and in the Congressional Record during any future floor consideration of this bill.

I look forward to working with you on this and other important legislation in the future.

Sincerely,

BENNIE G. THOMPSON,
Chairman.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, DC, September 2, 2020.

Chairman BENNIE G. THOMPSON,
Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR CHAIRMAN THOMPSON: I am writing to you concerning H.R. 5760, the ''Grid Security Research and Development Act,'' which was referred to the Committee on Science, Space, and Technology, and in addition to the Committee on Homeland Security on February 5, 2020.

I appreciate your willingness to work cooperatively on this bill. I recognize that the bill contains provisions that fall within the jurisdiction of the Committee on Homeland Security. I appreciate that your Committee will waive further consideration of H.R. 5760 and that this action is not a waiver of future jurisdictional claims by the Committee on Homeland Security over this subject matter.

I will make sure to include our exchange of letters in the legislative report for H.R. 5760 and in the Congressional Record. Thank you for your cooperation on this legislation.

Sincerely,

EDDIE BERNICE JOHNSON,
Chairwoman, Committee on Science, Space, and Technology.

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

Mr. Speaker, last week when the House considered the massive Clean Economy Jobs and Innovation Act, I expressed my disappointment with the partisan policies in the bill, with the rushed and irresponsible process of writing it, and, most of all, with the sheer number of missed bipartisan legislative opportunities it represents.

This week, I am glad to see that my friends across the aisle have taken heed of those words.

The Committee on Science, Space, and Technology has one of the best track records in Congress for passing productive, bipartisan legislation, and I am pleased to see us upholding that tradition once again.

H.R. 5760, the Grid Security Research and Development Act is a truly bipartisan Committee on Science, Space, and Technology product. It is sponsored by vice-chairman AMI BERA and Energy subcommittee Ranking Member RANDY WEBER. It has gone through regular order, and is the result of thoughtful consideration, careful analysis, and substantial debate. I support its passage today.

Currently, the U.S. energy sector and its aging electrical grid faces many critical challenges, like higher demand, vulnerability to cyberattacks, and increased integration of new energy sources. It is our job in Congress to set the priorities to meet these challenges and to focus our limited Federal funds where we can see the best return on investment.

To deliver effective solutions, we must take the long-term and big-picture approach. We must support early-stage research that will spur innovation over a broad range of energy applications and provide for R&D to mobilize and defend our critical energy infrastructure.

The bipartisan Grid Security Research and Development Act will strengthen our Nation's electric grid against rapidly changing technological challenges. It authorizes the Department of Energy's vital cybersecurity and emergency response R&D activities and directs DOE to work with relevant Federal agencies to develop cybersecurity best practices.

Through the committee markup process, we were able to improve this legislation by adding key research infrastructure provisions from my legislation, H.R. 5685, the Securing American Leadership in Science and Technology Act.

This provision requires the Secretary to carry out a program of research, development, and a demonstration of technologies and tools to help ensure the resilience and security of critical integrated grid infrastructures.

It also requires the Secretary to establish and operate a critical infrastructure test facility that allows for both physical and cyber performance testing to be conducted on large-scale infrastructure systems. This test facility will amplify and accelerate the high-priority research and development activities authorized in the original text and maximize the return on investment of taxpayers' dollars.

Mr. Speaker, I would like to take this opportunity to thank my good friends across the aisle for working with us to come to agreement on this provision and on this bill. I am glad to see we can come together to focus on our shared interest in improving U.S. national security and energy resilience for the next generation.

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

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

Mr. LUCAS. Mr. Speaker, I yield 5 minutes to the gentleman from Texas (Mr. WEBER), the ranking member of the Energy Subcommittee.

Mr. WEBER of Texas. Mr. Speaker, I thank the gentleman for yielding. I also thank Representative BERA for introducing this bill with me. I am proud to rise in support of H.R. 5760.

Mr. Speaker, cyber and physical threats to our electric grid are constantly evolving in technique and increasing in number. This challenge is magnified by its complexity. No two attacks are exactly the same.

Last year in the United States, the energy sector ranked ninth in industries most targeted by cyberattacks. In fact, IBM estimated that cyberattacks against vital energy sector technologies, like industrial control and operational systems, increased by more than 2,000 percent—2,000 percent.

Mr. Speaker, it is clear that we must be prepared to address this threat as we continue to build on the success of our clean energy future and long-term international competitiveness. Every single aspect of our daily lives in each economic sector in our Nation is dependent on the uninterrupted flow of power. I like to say that the things that make America great are the things that America makes.

How do we do that? With an uninterrupted, affordable flow of power.

Therefore, we must focus heavily on early-stage research into new technologies that will improve the resilience, the reliability, and the emergency response capabilities of our electric grid.

H.R. 5760 does that by authorizing a multi-agency research and development program to bolster the cyber and physical security capabilities of the energy sector.

It authorizes key Federal agencies, like the Department of Energy and the National Science Foundation, to support early-stage research, development, and demonstration activities that will advance critical cybersecurity technologies and enhance the security of energy sector information systems.

Mr. Speaker, I am also pleased to say, as the ranking member did, that this bill is truly bipartisan. We worked closely together to develop good legislation, and we included a key Committee on Science, Space, and Technology Republican priority; that is, a critical infrastructure research program and test facility.

This provision, originally offered by my good friend, Ranking Member LUCAS' bill, H.R. 5685, the Securing American Leadership in Science and Technology Act, was accepted as an amendment at committee markup.

In coordination with the Department of Defense and the Department of Homeland Security, the DOE-led research program and test facility will allow for U.S. researchers to conduct a variety of high-priority tests on critical infrastructure systems at the industry scale. This facility is a perfect example of the research asset that the Federal government is best suited to provide.

As recent events have shown us, it is not a question of if the U.S. power grid will face a significant physical or cyber threat, it is only a matter of when. In order to improve the cyber and physical security of our Nation's energy sector, we, in Congress, must continue to prioritize R&D to modernize and strengthen the national electricity system.

We can't agree on everything—I get that—especially when wish lists and partisan messaging exercises rule the day. However, when we identify our shared goals and work together in good faith, we can put together real legislation and find a path forward for the benefit of the American people.

Mr. Speaker, again, I thank Dr. BERA for introducing this legislation, and Members and staff of both sides of the aisle for working in a collaborative manner to reach a consensus on this standalone bill.

Mr. Speaker, I encourage my colleagues to support this legislation. There is real power in doing so.

Mr. BERA. Mr. Speaker, I, too, also want to recognize the bipartisan nature of this bill. It shows what we can do when we get together. I recognize the hard work of the staff from the Committee on Science, Space, and Technology.

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

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

Mr. Speaker, we must invest in the long-term, early-stage research that will strengthen our energy infrastructure against a range of emerging threats.

The Department of Energy is uniquely qualified to lead this endeavor, and the partnerships that exist between its national laboratory systems, universities, and industry has the potential to modernize and transform U.S. energy delivery systems.

H.R. 5760 authorizes the advanced grid security R&D activities that will make the future U.S. electrical grid reliable, resilient, and secure for all Americans.

I, again, thank my friends across the aisle for working with us on this bill. We need to come together and have serious conversations about how to make real progress on next-generation energy issues. I am glad to see us doing that today.

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

□ 1700

Mr. BERA. Mr. Speaker, I, once again, urge support of this commonsense, important legislation, and I yield back the balance of my time.

Ms. JOHNSON of Texas. Mr. Speaker, I rise today in support of H.R. 5760, the Grid Security Research and Development Act. I want to thank Mr. BERA for his leadership in introducing this bipartisan bill and for his commitment to developing legislation that will help strengthen America's electricity grid. I also want to thank my colleagues on the other side of the aisle who have recognized the importance of these investments and have joined me in supporting this important legislation.

The Grid Security Research and Development Act is updated version of a bill that Mr. BERA and I introduced, along with many of my Science Committee colleagues, in the previous two Congresses. This bill provides legislative guidance to the activities carried out by the recently established Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response by authorizing a cross-agency research and development program to advance electric grid cybersecurity and physical security. In particular, the bill authorizes activities on grid resilience and emergency response efforts, cybersecurity test beds, and education and workforce training for the energy sector.

The passage of this bill is particularly important now, as states all over the U.S. are experiencing unprecedented extreme weather events, ranging from historic hurricanes in Texas to the ongoing wildfires in California and Oregon. In California specifically, utilities are shutting off power to millions of customers when there are high winds in certain areas to prevent the onset of wildfires sparked by trees and other vegetation near critical grid infrastructure. This bill contains provisions to help address these important issues by directing the Department of Energy to conduct research on technologies to assist with the safe planning and execution of emergency power shutoffs, offer technical assistance on related topics, and establish a training program to improve grid resilience, among other provisions.

That's why I am proud to rise today in support of H.R. 5760. It would make important investments to improve the security and ensure the safety and resilience of our electric grid infrastructure. I also urge my colleagues to make a wise investment for our nation by joining me in supporting this bipartisan bill.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from California (Mr. BERA) that the House suspend the rules and pass the bill, H.R. 5760, 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.

REAFFIRMING THE HOUSE OF REPRESENTATIVES' COMMITMENT TO THE ORDERLY AND PEACEFUL TRANSFER OF POWER CALLED FOR IN THE CONSTITUTION OF THE UNITED STATES

Mr. SWALWELL of California. Mr. Speaker, I move to suspend the rules and agree to the resolution (H. Res. 1155) reaffirming the House of Representatives' commitment to the orderly and peaceful transfer of power called for in the Constitution of the United States, and for other purposes.

The Clerk read the title of the resolution.

The text of the resolution is as follows:

H. RES. 1155

Whereas the United States is founded on the principle that our Government derives its power from the consent of the governed and that the people have the right to change their elected leaders through elections;

Whereas our domestic tranquility, national security, general welfare, and civil liberties depend upon the peaceful and orderly transfer of power; and

Whereas any disruption occasioned by the transfer of the executive power could