I

116TH CONGRESS
2D SESSION

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.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 5, 2020

Mr. BERA (for himself and Mr. WEBER of Texas) introduced the following bill; which was referred to the Committee on Science, Space, and Technology, and in addition to the Committee on Homeland Security, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

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.

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, synchrophasors, 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 deteriorating electrical equipment on the transmission and distribution grid, including detection of spark ignition causing wildfires and risks of vegetation contact; and

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

''(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 electricity 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; and

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

''(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 utili-

ties, 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 analyses 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 features and 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); and

''(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) COLLABORATION.—In carrying out the program authorized in subsection (a), 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-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 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, com-

ponents, 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 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 Tech-

nology, 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 non-programmable 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 and private sector 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 title—

''(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.''.

○