AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

I

115TH CONGRESS
1ST SESSION

H. R. 4120

To provide for a comprehensive interdisciplinary research and development initiative to strengthen the capacity of the electricity sector to neutralize cyber attacks.

IN THE HOUSE OF REPRESENTATIVES

OCTOBER 25, 2017

Mr. BERA (for himself, Ms. EDDIE BERNICE JOHNSON of Texas, Mr. LIPINSKI, Ms. BONAMICI, and Ms. ROSEN) introduced the following bill; which was referred to the Committee on Science, Space, and Technology, and in addition to the Committees on Homeland Security, and Energy and Commerce, 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 and development initiative to strengthen the capacity of the electricity sector to neutralize cyber attacks.

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 Cybersecurity Research and Development Act''.

SEC. 2. FINDINGS.

Congress finds the following:

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

(2) Industrial control systems used in the electricity sector are essential to maintain reliable operations 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) There are substantial and important differences between cybersecurity approaches needed to protect information technology systems and industrial control systems.

(5) It is in the national interest for Federal agencies to invest in industrial control system cybersecurity research that facilitates private sector investment and the ability of the private sector to develop cybersecurity tools and products for control systems.

(6) The number of elements connecting to the electric grid is increasing, and designing cybersecurity into communication, data, and control systems when they are built is more effective than modifying

products after installation to meet cybersecurity goals.

(7) An understanding of human factors can be leveraged to understand the behavior of cyber threat actors, develop strategies to counter threat actors, improve industrial control system cybersecurity training programs, optimize the design of human-machine interfaces and cybersecurity tools, and increase the capacity of the electrical sector workforce to prevent attacks from gaining entry to industrial control systems.

SEC. 3. DEFINITIONS.

In this Act:

(1) CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—The term ''critical electric infrastructure information'' has the meaning given that term in section 215A(a)(3) of the Federal Power Act (16 U.S.C. 824a–1(a)(3)).

(2) CYBERSECURITY.—The term ''cybersecurity'' means a set of preventative measures to protect information from a digital device or system, including a device or system used to manage the electric grid, from being stolen, compromised, or used to carry out an attack.

(3) 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.

(4) 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.

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

(6) HUMAN-MACHINE INTERFACES.—The term ''human-machine interfaces'' means technologies that present information to an operator 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.

(7) SECRETARY.—The term ''Secretary'' means the Secretary of Energy.

(8) 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 for limited periods of time.

SEC. 4. ELECTRICITY SECTOR CYBERSECURITY RESEARCH, DEVELOPMENT, AND DEMONSTRATION PROGRAM.

(a) IN GENERAL.—The Secretary, in coordination with appropriate Federal agencies, the Electricity Subsector Coordinating Council, State, tribal, local, and territorial governments, private sector vendors, and other relevant stakeholders, shall carry out a research, development, and demonstration initiative to harden and mitigate the electric grid from the consequences of cyber attacks by increasing the cybersecurity capabilities of the elec-

tricity sector and accelerating the development of cybersecurity technologies and tools.

(b) DEPARTMENT OF ENERGY.—As part of the initiative described in subsection (a), the Secretary shall carry out activities to—

(1) identify cybersecurity risks to the communication and control systems within, and impacting, the electricity sector;

(2) develop methods and tools to rapidly detect cyber intruders and cyber incidents, including the use of data analytics techniques to validate and verify system behavior using multiple data streams reflecting the state of the system;

(3) assess emerging energy technology cybersecurity capabilities, and integrate cybersecurity features and protocols into the design, development, and deployment of emerging technologies, including renewable energy technologies;

(4) develop secure industrial control system protocols and identify vulnerabilities in existing protocols;

(5) work with manufacturers to build or retrofit security features and protocols into—

(A) communication and network systems and management processes;

(B) industrial control and energy management system devices, components, software, firmware, and hardware, including distributed control and management systems and building management systems;

(C) data storage systems and data management and analysis processes;

(D) generation, transmission, distribution, and energy storage technologies;

(E) automated and manually controlled devices and equipment for monitoring or managing frequency, voltage, and current;

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

(G) end user elements that connect to the grid, including—

(i) meters, synchrophasors, and other sensors;

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

(iii) distributed generation and energy storage technologies;

(iv) demand response technologies;

(v) home and building energy control systems;

(vi) electric and plug-in hybrid vehicles; and

(vii) other relevant devices, software, firmware, hardware, and distributed energy technologies; and

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

(6) improve the physical security of communication technologies and industrial control 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, and response;

(8) advance the capabilities and use of relevant interdisciplinary mathematical and computer simulation modeling and analysis methods;

(9) evaluate and understand the potential consequences of practices used to maintain the cybersecurity of information technology systems on the cybersecurity of industrial control systems;

(10) increase access to and the capabilities of existing cybersecurity test beds to simulate impacts of cyber attacks on industrial control system devices, components, software, and hardware; and

(11) reduce the cost of implementing effective cybersecurity technologies and tools in the electricity sector.

(c) NATIONAL SCIENCE FOUNDATION.—The National Science Foundation shall—

(1) support fundamental research to advance cybersecurity applications, technologies, and tools for industrial control systems, including incorporating 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 education and training for the industrial control system cybersecurity workforce, including through the Advanced Technological Education 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, in collaboration with the Department of Energy, experts in the private sector with the necessary clearances, and other relevant stakeholders, shall assess existing cybersecurity technologies and tools used in the defense industry and—

(1) identify technologies and tools that could be applied to meeting evolving 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. 5. TECHNICAL STANDARDS AND GUIDANCE DOCUMENTS FOR ELECTRICITY 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, private sector vendors, and other relevant stakeholders, shall coordinate the development of guidance documents for research and demonstration activities to improve the cybersecurity capabilities of the electricity 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 (published in September 2011);

(B) the Cybersecurity Procurement Language for Energy Delivery Systems (published by the Energy Sector Control Systems Working Group in April 2014), including developing guidance for—

(i) contracting with third parties to conduct vulnerability testing for industrial control systems;

(ii) contracting with third parties that will utilize transient devices to access industrial control or information technology systems; and

(iii) managing supply chain risks; and

(C) the Electricity Subsector Cybersecurity Capability Maturity Model (published by the Department of Energy in February 2014), including the development of—

(i) metrics to measure changes in cybersecurity capabilities and assess the potential for metrics to drive unexpected behavioral changes that would reduce security; and

(ii) an analysis of incentive mechanisms and their potential to increase investments in cybersecurity;

(2) develop voluntary guidance to improve forensic analyses capabilities, including—

(A) developing standardized terminology and monitoring processes;

(B) identifying minimum data needed; and

(C) 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, National Institute of Standards and Technology, and stakeholders to develop a mechanism to anonymize, aggregate, and share the testing results from cybersecurity industrial control system test beds to facilitate technology improvements by public and private sector researchers.

(b) CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—Information provided to Federal agencies for the purposes of carrying out subsection (a) shall be considered critical electric infrastructure information and provided the protections established in section 10.

(c) STANDARDS.—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) voluntary, consensus-based technical standards to improve cybersecurity for—

(A) emerging energy technologies;

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

(C) electric vehicles; and

(D) other technologies and devices that connect to the electric grid that can affect voltage stability;

(2) recommended cybersecurity features and requirements that can be used by the private sector to design and build interoperable cybersecurity features into—

(A) devices and components;

(B) software and hardware; and

(C) other technologies that connect to the electric grid; and

(3) voluntary standards for test beds and test bed methodologies that will enable reproducible testing of industrial control system devices, components, software, and hardware across test beds.

(d) REGULATORY AUTHORITY.—Subsection (c) shall not be construed to authorize regulatory actions that would duplicate or conflict with regulatory requirements, mandatory standards, or related processes under any other provision of Federal law.

SEC. 6. VULNERABILITY TESTING AND TECHNICAL ASSISTANCE TO INCREASE CYBERRESILIENCE.

(a) IN GENERAL.—The Secretary shall—

(1) collaborate with electricity sector asset owners and operators in the private sector, leveraging

the research facilities and expertise of the National Laboratories, to—

(A) utilize a range of methods, including voluntary vulnerability testing and red team-blue team exercises, to identify vulnerabilities in physical and cyber systems;

(B) develop cybersecurity risk assessment tools and provide confidential analyses and recommendations to participating stakeholders;

(C) work with stakeholders to develop methods to share anonymized and aggregated results in a format that enables the electricity sector, researchers, and the private sector to advance cybersecurity efforts, technologies, and tools; and

(D) leverage the unique strengths and expertise of the National Laboratories and Federal agencies;

(2) collaborate with relevant stakeholders to—

(A) identify information, research, staff training, and analysis tools needed to evaluate industrial control system cybersecurity issues and challenges in the electricity sector; and

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

(3) collaborate with and support electricity sector trade organizations and their research agencies to improve the cybersecurity of industrial control systems used by members and stakeholders; and

(4) collaborate with tribal governments to—

(A) identify information, research, and analysis tools needed by tribal governments to increase the industrial control system cybersecurity of electricity assets within their jurisdiction; and

(B) facilitate the sharing of information and the development of tools needed to ensure the cybersecurity of tribal electricity assets and systems.

(b) CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—Information provided to Federal agencies for the purposes of carrying out subsection (a)(1)(C) shall be considered critical electric infrastructure information and provided the protections established in section 10.

SEC. 7. EDUCATION AND WORKFORCE TRAINING RESEARCH AND STANDARDS.

(a) DEPARTMENT OF ENERGY.—The Secretary shall—

(1) utilize human factors research and other methods to identify core skills used by electricity sector industrial control systems cybersecurity professionals; and

(2) develop assessment methods and tools to identify existing personnel that show competence in the core skills identified under paragraph (1).

(b) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.—The Director of the National Institute of Standards and Technology shall—

(1) develop voluntary, innovative industrial control systems cybersecurity training and retraining standards, lessons, and recommendations for the electricity sector that minimize duplication of cybersecurity compliance training programs; and

(2) maintain a public database of industrial control systems cybersecurity education, training, and certification programs.

SEC. 8. INTERAGENCY COORDINATION AND STRATEGIC PLAN FOR ELECTRICITY SECTOR CYBERSECURITY RESEARCH.

(a) DUTIES.—The Energy Sector Government Coordinating Council shall—

(1) review the most recent version of the Roadmap to Achieve Energy Delivery Systems Cybersecurity and identify crosscutting energy grid cybersecurity research needs and opportunities for collaboration among Federal agencies and between Federal agencies and other relevant stakeholders;

(2) identify interdisciplinary research, technology, and tools that can be applied to industrial control system cybersecurity challenges in the electricity sector;

(3) identify technology transfer opportunities to accelerate the development and commercial application of novel industrial control system cybersecurity technologies, systems, and processes; and

(4) develop a coordinated Interagency Strategic Plan to advance cybersecurity capabilities for industrial control systems used in the electricity sector that builds on the Roadmap to Achieve Energy Delivery Systems in Cybersecurity.

(b) 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 this Act.

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

(A) an analysis of how existing cybersecurity research efforts conducted by member agencies are coordinated and can complement and advance the goals of the Roadmap to Achieve Energy Delivery Systems Cybersecurity;

(B) recommendations for prioritized research efforts that could contribute to advancing the cybersecurity of electricity sector industrial control systems;

(C) a description of how existing and proposed public and private sector research efforts address the topics described in paragraph (3); and

(D) a description of needed support for workforce training in this area.

(3) CONSIDERATION.—In developing the Interagency Strategic Plan, 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 protocols, devices, components, technologies, and tools;

(C) opportunities for Small Business Innovation Research (SBIR) and other technology transfer programs to facilitate private sector development of industrial control system cybersecurity protocols, devices, components, technologies, and tools;

(D) broader applications of the work done by relevant Federal agencies to advance the cybersecurity of industrial control systems used by other sectors; 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) MEMBERSHIP.—For the purposes of carrying out this section, the Energy Sector Government Coordinating

Council shall include representatives from Federal agencies with expertise in industrial control systems cybersecurity, information technology cybersecurity, 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. The Chair shall consider including at least one employee designated by the head of each of the following agencies:

(1) In the Department of Energy—

(A) the Office of Electricity Delivery and Energy Reliability;

(B) the Office of Science's Advanced Scientific Computing Research program;

(C) the Office of Small Business Innovation Research/Small Business Technology Transfer programs;

(D) the Office of Technology Transitions; and

(E) other offices considered appropriate by the Secretary.

(2) The National Science Foundation.

(3) The Department of Homeland Security's Science and Technology Directorate.

(4) The National Institute of Standards and Technology.

(5) The National Aeronautics and Space Administration's Human Research Program.

(6) The Office of Science and Technology Policy.

(7) The Federal Energy Regulatory Commission.

SEC. 9. REPORTS TO CONGRESS.

(a) IDENTIFICATION OF COMMON FACTORS IN CYBER ATTACKS.—

(1) STUDY.—The Secretary, in collaboration with the Secretary of Homeland Security, other appropriate Federal agencies, and energy sector stakeholders, shall conduct a study to analyze cyber attacks on electricity sector industrial control systems and identify cost-effective opportunities to improve cybersecurity.

(2) CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—Incident data provided to Federal agencies for the purposes of carrying out this subsection shall be considered critical electric infrastructure information and provided the protections established in section 10.

(3) CONTENT.—The study shall—

(A) summarize cyber incident data provided to the Secretary by relevant Federal agencies and energy sector stakeholders;

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

(C) identify the points where human behavior played a critical role in maintaining or compromising the security of the system;

(D) recommend—

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

(ii) changes to processes or operational procedures that do not require a change in human behavior; and

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

(E) evaluate existing engineering and technical design criteria and guidelines that incorporate human factors research findings, and recommend criteria and guidelines for industrial

control system cybersecurity tools that can be used to develop procurement guidance, including guidance for alarms, displays, and layouts.

(4) CONSULTATION.—In conducting the study, the Secretary shall consult with electricity sector stakeholders, professionals with expertise in human factors research, private sector industrial control system vendors, and other relevant parties.

(5) REPORT.—Not later than 24 months after the date of enactment of this Act, the Secretary shall submit to the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Energy and Natural Resources of the Senate a report on the results of the study, including the findings of the Secretary on each of the items described in paragraph (3).

(b) BALANCING RISKS, SECURITY, AND MODERNIZATION OF INDUSTRIAL SYSTEMS.—

(1) STUDY.—The Secretary, in collaboration with the National Institute of Standards and Technology, other Federal agencies, and electricity sector stakeholders, shall examine the risks associated with increasing penetration of digital technologies in operational networks.

(2) CONTENT.—The study shall—

(A) evaluate the relative qualitative risks and benefits of various design and architecture options for electricity sector industrial control systems, including consideration of—

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

(ii) different communication technologies used to move 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; and

(v) increased redundancy using dissimilar cybersecurity technologies;

(B) recommend methods or metrics to document changes in risks associated with system designs and architectures;

(C) provide recommendations for research, development, demonstration, and commercial application activities to address issues raised in subparagraphs (A) and (B); and

(D) recommend guidance to minimize overall system risks.

(3) CONSULTATION.—In conducting the study, the Secretary shall consult with electricity sector stakeholders, academic and private sector researchers, private sector industrial control system vendors, and other relevant parties.

(4) REPORT.—Not later than 24 months after the date of enactment of this Act, the Secretary shall submit to the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Energy and Natural Resources of the Senate a report on the results of the study, including the findings of the Secretary on each of the items described in paragraph (2).

SEC. 10. PROTECTION OF CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.

Any Federal agency that produces information or has information made available to it in the course of carrying out this Act shall determine whether to designate any such information as critical electric infrastructure information. Critical electric infrastructure information—

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

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

SEC. 11. AUTHORIZATION OF APPROPRIATIONS.

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

(1) $65,000,000 for fiscal year 2018;

(2) $68,250,000 for fiscal year 2019;

(3) $71,662,500 for fiscal year 2020;

(4) $75,245,625 for fiscal year 2021; and

(5) $79,007,906 for fiscal year 2022.

○