[DISCUSSION DRAFT]

118TH CONGRESS
1ST SESSION

H. R. _____

To [provide for grid security], and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M_. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To [provide for grid security], 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 "[_____ Act of 2023]".

SEC. 2. [GRID SECURITY].

(a) IN GENERAL.—Title VIII of division Z of the Consolidated Appropriations Act, 2021 (Public Law 116–260) is amended—

(1) by redesignating sections 8013 through 8015 as sections 8022 through 8024, respectively; and

(2) by inserting after section 8012 the following:

"SEC. 8013. ENERGY SECTOR SECURITY RESEARCH, DEVELOPMENT, AND DEMONSTRATION PROGRAM.

''(a) IN GENERAL.—The Secretary, in coordination with the heads of 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, subtransmission and transmission grids, and associated supply chains, 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 technology and operational technology within, and impacting, the electricity sector, energy systems, and energy infrastructure;

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

''(3) develop methods and tools for distributed and collaborative cybersecurity defense and analysis that can be deployed across the electric sector to maximize scale and provide increased automation;

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

''(5) identify existing vulnerabilities in intelligent electronic devices, advanced analytics systems, information systems, control and protection devices, and distributed generation sources;

''(6) work with relevant entities to develop algorithms, methodologies, technologies, or other 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 controlling the electric grid;

''(D) technologies used to synchronize time;

''(E) power system delivery and end user systems and devices that exchange information with grid systems or respond to grid conditions, 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;

"(vii) electrified aerospace mobility;

"(viii) internet of things and the industrial internet of things; and

"(ix) other relevant devices, software, firmware, and hardware; and

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

"(6) develop technologies, including information technologies and operational technologies, that improve the physical security of the electric grid, 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 ongoing monitoring, maintenance, and updates of these technologies and tools, in the energy sector.

''(c) NATIONAL SCIENCE FOUNDATION.—The Director of the National Science Foundation, in coordination with the heads of 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 that support the electric grid and energy systems, including interdisciplinary research in—

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

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

"(C) advanced data analytical methods, mathematics, computer coding, and algorithms; and

"(D) machine learning, artificial intelligence, and federated learning 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 Secretary of Homeland Security, acting through the Science and Technology Directorate shall coordinate with the Secretary of Energy, the private sector, and other relevant stakeholders, to research existing cybersecurity tech-

nologies 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. 8014. 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 (d) on a competitive basis to conduct research and development with the purpose of

improving the resilience and reliability of the electric grid by—

''(1) developing methods, data, and tools to improve community and governmental preparation for an emergency response to widespread, long-duration electricity outages, including through the use of energy efficiency, energy storage, demand response, 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 better plan for cross-sector dependencies among critical infrastructures such as electricity, natural gas, telecommunications, and transportation as they relate to cyber and physical threats, vulnerabilities, and response;

''(4) 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;

''(5) developing technologies and capabilities to withstand and manage the current and projected impact of the changing climate on energy sector infra-

structure, including extreme weather events, other natural disasters, and wildfires;

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

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

''(8) developing tools that can estimate the economic, health, safety, and other impacts of widespread, long-duration electricity outages and interruptions;

''(9) develop guidance for operational contingency plans when time synchronization technologies, are compromised; and

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

''(c) CONCURRENT AND CO-LOCATED DISASTERS.—In carrying out the program under subsection (a), the Secretary shall support research and development on tools, techniques, and technologies for improving electric grid and energy sector safety and resilience in the event of multiple simultaneous or co-located weather or climate events leading to extreme conditions, such as extreme wind, wildfires, extreme cold, and extreme heat, or natural disasters co-incident with cyberattacks.

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

''(1) an institution of higher education, which includes a historically Black college or university or a minority-serving institution;

''(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 paragraphs (1) through (7); and

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

''(e) RELEVANT ACTIVITIES.—Grants awarded under subsections (b) and (c) shall include funding for research and development activities related to the purpose described in subsections (b) and (c), including—

''(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 widespread, long-duration electricity interruptions to identify common elements and best practices for electricity restoration, prevention of future disruptions and the mitigation of impacts to electricity infrastructure;

''(4) development of—

''(A) advanced monitoring, analytics, operation, planning, and controls of electric grid and interdependent systems to improve electric grid resilience; and

''(B) independent verification and validation methodologies, in coordination with the National Institute of Standards and Tech-

nology, to address the potential cybersecurity vulnerabilities of electric grid systems and of the technologies identified in subparagraph (A) of this paragraph;

''(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 evaluate and maintain cybersecurity during restoration of energy sector infrastructure and operation;

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

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

''(f) 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;

''(E) the development of tools and technologies to coordinate data across relevant entities to promote resilience and wildfire prevention in the planning, design, construction, oper-

ation, 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 grid enhancing technologies, 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 subsection 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 subsection shall authorize the Secretary to require any entity to adopt any model, tool, technology, plan, analysis, or assessment.

"SEC. 8015. BEST PRACTICES AND GUIDANCE DOCUMENTS FOR ENERGY SECTOR CYBERSECURITY RESEARCH.

"(a) IN GENERAL.—The Secretary, in coordination with the heads of appropriate Federal agencies, the Electricity Subsector Coordinating Council, standards development organizations, State, Tribal, local, and territorial governments, the national laboratories, the private sector, public utility commissions, and other relevant stakeholders, shall coordinate the development of guidance documents for research, development, and demonstration ac-

tivities to improve the cybersecurity capabilities of the energy sector through participating agencies. As part of these activities, the Secretary, in coordination with relevant Federal agencies, shall—

"(1) facilitate stakeholder involvement to update—

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

"(B) the Report on Cybersecurity of Electrical Distribution Systems;

"(C) 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

"(D) the Electricity Subsector Cybersecurity Capability Maturity Model, including the

development of metrics to measure changes in cybersecurity readiness;

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

"(A) developing standardized terminology and normalized baseline monitoring processes;

"(B) utilizing human factors research to develop more effective procedures for responding, logging, and mitigating incident events; and

"(C) developing standardized approaches to reporting and sharing cyber threat information stemming from observation of cyber activity; 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, the Director of the Cybersecurity and Infrastructure Security Agency, and the heads of

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 energy storage technologies, and other distributed energy resources;

"(C) distributed energy resource aggregators and other distributed generation service providers;

"(D) electric vehicles and electric vehicle charging stations; and

"(E) 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 in-

formation 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. 8016. VULNERABILITY TESTING AND TECHNICAL ASSISTANCE TO IMPROVE CYBERSECURITY.

''The Secretary shall—

''(1) coordinate with the heads of appropriate Federal agencies and 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, including advanced control and artificial intelligence-based algorithms, 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 appropriate Federal agencies and stakeholders to develop methods and tools 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, automation tools, 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) coordinate 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. 8017. CYBERSECURITY 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, faculty, 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 for the energy sector;

''(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 energy sector 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 coordinate with appropriate Federal agencies and 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. 8018. INTERAGENCY COORDINATION AND STRATEGIC PLAN FOR ENERGY SECTOR CYBERSECURITY RESEARCH.

''(a) DUTIES.—The Secretary, in coordination with the heads of appropriate Federal agencies and the Energy Sector Government Coordinating Council, shall—

''(1) review the updated 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 appropriate Federal agencies and 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 cy-

bersecurity 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, advanced data analytical methods, or other disciplines considered appropriate by the Council Chair.

''SEC. 8019. REPORT TO CONGRESS.

''(a) 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 conduct a study that—

''(1) analyzes processes, operational procedures, and other factors common among physical and cyber attacks;

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

''(3) recommends—

''(A) 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

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

''(4) evaluates 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;

''(5) evaluates the physical and 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—

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

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

"(C) automated and human-in-the-loop devices and technologies;

"(D) programmable versus nonprogrammable devices and technologies;

"(E) increased redundancy using dissimilar cybersecurity technologies; and

"(F) grid architectures that use autonomous functions to limit control vulnerabilities;

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

"(7) identifies cost-effective opportunities to improve physical cybersecurity.

"(b) CONSULTATION.—In conducting the study, the Secretary shall consult with energy sector stakeholders,

academic researchers, the private sector, and other relevant stakeholders.

''(c) 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. 8020. 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 grid infrastructures.

''(b) CRITICAL INFRASTRUCTURE DEFINED.—In this section, 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) ENERGY SECTOR CRITICAL INFRASTRUCTURE TEST FACILITY.—In carrying out the program under subsection (a), the Secretary, in consultation with other appropriate Federal agencies, shall establish and operate an Energy Sector 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 energy sector 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. 8021. DEFINITIONS.

''In this title:

''(1) 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.

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

''(3) DEPARTMENT.—The term 'Department' means the Department Of Energy.

''(4) ELECTRICITY SUBSECTOR COORDINATING COUNCIL.—The term 'Electricity Subsector Coordinating Council' means the self-organized, self-governed council consisting of senior industry represent-

atives 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) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The term 'historically Black college or university' has the meaning given the term 'part B institution' in section 322(2) of the Higher Education Act of 1965 (29 U.S.C. 106(2)).

''(7) 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.

''(8) 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.

''(9) 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.

''(10) MINORITY-SERVING INSTITUTION.—The term 'minority-serving institution' means an eligible institution under section 371(a) of the Higher Education Act of 1965 (20 U.S.C. 1067q(a)).

''(11) 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).

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

''(13) 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).

''(14) 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.

''(15) LONG-DURATION.—The term 'long-duration' refers to an event lasting longer than 24 hours.

''(16) INTERNET OF THINGS.—The term 'internet of things' means the network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information.

''(17) INDUSTRIAL INTERNET OF THINGS.—The term 'industrial internet of things' means the sensors, instruments, machines, and other devices that are networked together and use Internet connectivity to enhance industrial and manufacturing business processes and applications.''.

(b) CONFORMING AMENDMENTS.—Section 101(b) of division Z of the Consolidated Appropriations Act, 2021

(Public Law 116–260) is amended in the table of contents—

(1) in the matter relating to 8013, by striking ''8013'' and inserting ''8022'';

(2) in the matter relating to 8014, by striking ''8014'' and inserting ''8023'';

(3) in the matter relating to 8015, by striking ''8015'' and inserting ''8024''; and

(4) by adding after the matter relating to section 8012 the following: