

117TH CONGRESS
1ST SESSION

H. R. 4939

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

AUGUST 6, 2021

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Grid Security Research
5 and Development Act”.

1 **SEC. 2. FINDINGS.**

2 Congress finds the following:

3 (1) The Nation, and every critical infrastruc-
4 ture sector, depends on reliable electricity.

5 (2) Intelligent electronic devices, advanced ana-
6 lytics, and information systems used across the en-
7 ergy sector are essential to maintaining reliable op-
8 eration of the electric grid.

9 (3) The cybersecurity threat landscape is con-
10 stantly changing and attacker capabilities are ad-
11 vancing rapidly, requiring ongoing modifications, ad-
12 vancements, and investments in technologies, proce-
13 dures, and workforce development to maintain secu-
14 rity.

15 (4) It is in the national interest for Federal
16 agencies to invest in innovative cybersecurity re-
17 search that informs and facilitates private sector in-
18 vestment and use of new and advanced cybersecurity
19 tools and procedures to protect information systems.

20 (5) The number of devices and systems con-
21 necting to the electric grid is increasing, and inte-
22 grating cybersecurity protections into information
23 systems when they are designed and built is more ef-
24 fective than modifying products after installation to
25 meet cybersecurity goals.

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

9 **SEC. 3. AMENDMENT TO DIVISION Z OF THE CONSOLI-**
10 **DATED APPROPRIATIONS ACT, 2021.**

11 Title VIII of division Z of the Consolidated Appro-
12 priations Act, 2021 (Public Law 116–260) is amended by
13 inserting after section 8012 the following:

14 **“SEC. 8013. ENERGY SECTOR SECURITY RESEARCH, DEVEL-**
15 **OPMENT, AND DEMONSTRATION PROGRAM.**

16 “(a) IN GENERAL.—The Secretary, in coordination
17 with appropriate Federal agencies, the Electricity Sub-
18 sector Coordinating Council, the Electric Reliability Orga-
19 nization, State, tribal, local, and territorial governments,
20 the private sector, and other relevant stakeholders, shall
21 carry out a research, development, and demonstration pro-
22 gram to protect the electric grid and energy systems, in-
23 cluding assets connected to the distribution grid, and asso-
24 ciated supply chains, from cyber and physical attacks by
25 increasing the cyber and physical security capabilities of

1 the energy sector and accelerating the development of rel-
2 evant technologies and tools.

3 “(b) DEPARTMENT OF ENERGY.—As part of the ini-
4 tiative described in subsection (a), the Secretary shall
5 award research, development, and demonstration grants
6 to—

7 “(1) identify cybersecurity risks to information
8 technology and operational technology within, and
9 impacting, the electricity sector, energy systems, and
10 energy infrastructure;

11 “(2) develop methods and tools to rapidly detect
12 cyber intrusions and cyber incidents, including
13 through the use of data and big data analytics tech-
14 niques, such as intrusion detection, and security in-
15 formation and event management systems, to vali-
16 date and verify system behavior;

17 “(3) assess emerging cybersecurity capabilities
18 that could be applied to energy systems and develop
19 technologies that integrate cybersecurity features
20 and procedures into the design and development of
21 existing and emerging grid technologies, including
22 renewable energy, storage, and demand-side manage-
23 ment technologies;

1 “(4) identify existing vulnerabilities in intel-
2 ligent electronic devices, advanced analytics systems,
3 and information systems;

4 “(5) work with relevant entities to develop tech-
5 nologies or concepts that build or retrofit cybersecu-
6 rity features and procedures into—

7 “(A) information and energy management
8 system devices, components, software, firmware,
9 and hardware, including distributed control and
10 management systems, and building manage-
11 ment systems;

12 “(B) data storage systems, data manage-
13 ment systems, and data analysis processes;

14 “(C) automated and manually controlled
15 devices and equipment for monitoring and sta-
16 bilizing the electric grid;

17 “(D) technologies used to synchronize time
18 and develop guidance for operational contin-
19 gency plans when time synchronization tech-
20 nologies, are compromised;

21 “(E) power system delivery and end user
22 systems and devices that connect to the grid,
23 including—

24 “(i) meters, phasor measurement
25 units, and other sensors;

1 “(ii) distribution automation tech-
2 nologies, smart inverters, and other grid
3 control technologies;

4 “(iii) distributed generation, energy
5 storage, and other distributed energy tech-
6 nologies;

7 “(iv) demand response technologies;

8 “(v) home and building energy man-
9 agement and control systems;

10 “(vi) electric and plug-in hybrid vehi-
11 cles and electric vehicle charging systems;

12 and

13 “(vii) other relevant devices, software,
14 firmware, and hardware; and

15 “(F) the supply chain of electric grid man-
16 agement system components;

17 “(6) develop technologies, including information
18 technologies and operational technologies, that im-
19 prove the physical security of the electric grid, in-
20 cluding remote assets;

21 “(7) integrate human factors research into the
22 design and development of advanced tools and proc-
23 esses for dynamic monitoring, detection, protection,
24 mitigation, response, and cyber situational aware-
25 ness;

1 “(8) evaluate and understand the potential con-
2 sequences of practices used to maintain the cyberse-
3 curity of information systems and intelligent elec-
4 tronic devices;

5 “(9) develop or expand the capabilities of exist-
6 ing cybersecurity test beds to simulate impacts of
7 cyber attacks and combined cyber-physical attacks
8 on information systems and electronic devices, in-
9 cluding by increasing access to existing and emerg-
10 ing test beds for cooperative utilities, utilities owned
11 by a political subdivision of a State, such as municipi-
12 pally owned electric utilities, and other relevant
13 stakeholders; and

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

18 “(c) NATIONAL SCIENCE FOUNDATION.—The Na-
19 tional Science Foundation, in coordination with other Fed-
20 eral agencies as appropriate, shall through its cybersecu-
21 rity research and development programs—

22 “(1) support basic research to advance knowl-
23 edge, applications, technologies, and tools to
24 strengthen the cybersecurity of information systems

1 that support the electric grid and energy systems,
2 including interdisciplinary research in—

3 “(A) evolutionary systems, theories, mathe-
4 matics, and models;

5 “(B) economic and financial theories,
6 mathematics, and models; and

7 “(C) big data analytical methods, mathe-
8 matics, computer coding, and algorithms; and

9 “(2) support cybersecurity education and train-
10 ing focused on information systems for the electric
11 grid and energy workforce, including through the
12 Advanced Technological Education program, the
13 Cybercorps program, graduate research fellowships,
14 and other appropriate programs.

15 “(d) DEPARTMENT OF HOMELAND SECURITY
16 SCIENCE AND TECHNOLOGY DIRECTORATE.—The Science
17 and Technology Directorate of the Department of Home-
18 land Security shall coordinate with the Department of En-
19 ergy, the private sector, and other relevant stakeholders,
20 to research existing cybersecurity technologies and tools
21 used in the defense industry in order to—

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

24 “(2) develop a research strategy that incor-
25 porates human factors research findings to guide the

1 modification of defense industry cybersecurity tools
2 for use in the civilian sector;

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

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

9 **“SEC. 8014. GRID RESILIENCE AND EMERGENCY RESPONSE.**

10 “(a) IN GENERAL.—Not later than 180 days after
11 the enactment of the Grid Security Research and Develop-
12 ment Act, the Secretary shall establish a research, devel-
13 opment, and demonstration program to enhance resilience
14 and strengthen emergency response and management per-
15 taining to the energy sector.

16 “(b) GRANTS.—The Secretary shall award grants to
17 eligible entities under subsection (d) on a competitive basis
18 to conduct research and development with the purpose of
19 improving the resilience and reliability of the electric grid
20 by—

21 “(1) developing methods to improve community
22 and governmental preparation for and emergency re-
23 sponse to large-area, long-duration electricity inter-
24 ruptions, including through the use of energy effi-

1 ciency, storage, and distributed generation tech-
2 nologies;

3 “(2) developing tools to help utilities and com-
4 munities ensure the continuous delivery of electricity
5 to critical facilities;

6 “(3) developing tools to improve coordination
7 between utilities and relevant Federal agencies to
8 enable communication, information-sharing, and sit-
9 uational awareness in the event of a physical or
10 cyber-attack on the electric grid;

11 “(4) developing technologies and capabilities to
12 withstand and address the current and projected im-
13 pact of the changing climate on energy sector infra-
14 structure, including extreme weather events, other
15 natural disasters, and wildfires;

16 “(5) developing technologies capable of early
17 detection of malfunctioning electrical equipment on
18 the transmission and distribution grid, including de-
19 tection of spark ignition causing wildfires and risks
20 of vegetation contact;

21 “(6) assessing upgrades and additions needed
22 to energy sector infrastructure due to projected
23 changes in the energy generation mix and energy de-
24 mand;

1 “(7) upgrading tools used to estimate the costs
2 of outages longer than 24 hours; and

3 “(8) developing tools and technologies to assist
4 with the planning, safe execution of, and safe and
5 timely restoration of power after cyber and physical
6 attacks, natural disasters, and emergency power
7 shut offs, such as those conducted to reduce risks of
8 wildfires started by grid infrastructure.

9 “(c) CONCURRENT AND CO-LOCATED DISASTERS.—
10 In carrying out the program under subsection (a), the Sec-
11 retary shall support research and development on tools,
12 techniques, and technologies for improving electric grid
13 and energy sector safety and resilience in the event of mul-
14 tiple simultaneous or co-located weather or climate events
15 leading to extreme conditions, such as extreme wind,
16 wildfires, extreme cold, and extreme heat.

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

19 “(1) an institution of higher education, includ-
20 ing a historically Black college or university or a mi-
21 nority-serving institution;

22 “(2) a nonprofit organization;

23 “(3) a National Laboratory;

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

25 “(5) an electric utility or electric cooperative;

1 “(6) a retail service provider of electricity;

2 “(7) a private commercial entity;

3 “(8) a partnership or consortium of 2 or more
4 entities described in paragraphs (1) through (7); and

5 “(9) any other entities the Secretary deems ap-
6 propriate.

7 “(e) RELEVANT ACTIVITIES.—Grants awarded under
8 subsection (b) shall include funding for research and de-
9 velopment activities related to the purpose described in
10 subsection (b), such as—

11 “(1) development of technologies to use distrib-
12 uted energy resources, such as solar photovoltaics,
13 energy storage systems, electric vehicles, and micro-
14 grids, to improve grid and critical end-user resil-
15 ience;

16 “(2) analysis of non-technical barriers to great-
17 er integration and use of technologies on the dis-
18 tribution grid;

19 “(3) analysis of past large-area, long-duration
20 electricity interruptions to identify common elements
21 and best practices for electricity restoration, mitiga-
22 tion, and prevention of future disruptions;

23 “(4) development of—

1 “(A) advanced monitoring, analytics, oper-
2 ation, and controls of electric grid systems to
3 improve electric grid resilience; and

4 “(B) independent verification and valida-
5 tion methodologies, in coordination with the
6 National Institute of Standards and Tech-
7 nology, to address the potential cybersecurity
8 vulnerabilities of the technologies identified in
9 subparagraph (A) of this paragraph;

10 “(5) analysis of technologies, methods, and con-
11 cepts that can improve community resilience and
12 survivability of frequent or long-duration power out-
13 ages;

14 “(6) development of methodologies to maintain
15 cybersecurity during restoration of energy sector in-
16 frastructure and operation;

17 “(7) development of advanced power flow con-
18 trol systems and components to improve electric grid
19 resilience; and

20 “(8) any other relevant activities determined by
21 the Secretary.

22 “(f) TECHNICAL ASSISTANCE.—

23 “(1) IN GENERAL.—The Secretary shall provide
24 technical assistance to eligible entities for the com-
25 mercial application of technologies to improve the re-

1 silience of the electric grid and commercial applica-
2 tion of technologies to help entities develop plans for
3 preventing and recovering from various power out-
4 age scenarios at the local, regional, and State level.

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

9 “(A) the commercial application of tech-
10 nologies developed from the grant program es-
11 tablished in subsection (b), including coopera-
12 tive utilities and utilities owned by a political
13 subdivision of a State, such as municipally
14 owned electric utilities;

15 “(B) the development of methods to
16 strengthen or otherwise mitigate adverse im-
17 pacts on electric grid infrastructure against
18 natural hazards;

19 “(C) the use of Department data and mod-
20 eling tools for various purposes;

21 “(D) a resource assessment and analysis of
22 future demand and distribution requirements,
23 including development of advanced grid archi-
24 tectures and risk analysis;

1 “(E) the development of tools and tech-
2 nologies to coordinate data across relevant enti-
3 ties to promote resilience and wildfire preven-
4 tion in the planning, design, construction, oper-
5 ation, and maintenance of transmission infra-
6 structure;

7 “(F) analysis to predict the likelihood of
8 extreme weather events to inform the planning,
9 design, construction, operation, and mainte-
10 nance of transmission infrastructure in con-
11 sultation with the National Oceanic and Atmos-
12 pheric Administration; and

13 “(G) the commercial application of rel-
14 evant technologies, such as distributed energy
15 resources, microgrids, or other energy tech-
16 nologies, to establish backup power for users or
17 facilities affected by emergency power shutoffs.

18 “(3) ELIGIBLE ENTITIES.—The entities eligible
19 to receive technical assistance for commercial appli-
20 cation of technologies under this subsection in-
21 clude—

22 “(A) representatives of all sectors of the
23 electric power industry, including electric utili-
24 ties, trade organizations, and transmission and

1 distribution system organizations, owners, and
2 operators;

3 “(B) State and local governments and reg-
4 ulatory authorities, including public utility com-
5 missions;

6 “(C) tribal and Alaska Native govern-
7 mental entities;

8 “(D) partnerships among entities under
9 subparagraphs (A) through (C);

10 “(E) regional partnerships; and

11 “(F) any other entities the Secretary
12 deems appropriate.

13 “(4) AUTHORITY.—Nothing in this subsection
14 shall authorize the Secretary to require any entity to
15 adopt any model, tool, technology, plan, analysis, or
16 assessment.

17 **“SEC. 8015. BEST PRACTICES AND GUIDANCE DOCUMENTS**
18 **FOR ENERGY SECTOR CYBERSECURITY RE-**
19 **SEARCH.**

20 “(a) IN GENERAL.—The Secretary, in coordination
21 with appropriate Federal agencies, the Electricity Sub-
22 sector Coordinating Council, standards development orga-
23 nizations, State, tribal, local, and territorial governments,
24 the private sector, public utility commissions, and other
25 relevant stakeholders, shall coordinate the development of

1 guidance documents for research, development, and dem-
2 onstration activities to improve the cybersecurity capabili-
3 ties of the energy sector through participating agencies.
4 As part of these activities, the Secretary, in consultation
5 with relevant Federal agencies, shall—

6 “(1) facilitate stakeholder involvement to up-
7 date—

8 “(A) the Roadmap to Achieve Energy De-
9 livery Systems Cybersecurity;

10 “(B) the Cybersecurity Procurement Lan-
11 guage for Energy Delivery Systems, including
12 developing guidance for—

13 “(i) contracting with third parties to
14 conduct vulnerability testing for informa-
15 tion systems used across the energy pro-
16 duction, delivery, storage, and end use sys-
17 tems;

18 “(ii) contracting with third parties
19 that utilize transient devices to access in-
20 formation systems; and

21 “(iii) managing supply chain risks;
22 and

23 “(C) the Electricity Subsector Cybersecu-
24 rity Capability Maturity Model, including the

1 development of metrics to measure changes in
2 cybersecurity readiness; and

3 “(2) develop voluntary guidance to improve dig-
4 ital forensic analysis capabilities, including—

5 “(A) developing standardized terminology
6 and monitoring processes; and

7 “(B) utilizing human factors research to
8 develop more effective procedures for logging
9 incident events; and

10 “(3) work with the National Science Founda-
11 tion, Department of Homeland Security, and stake-
12 holders to develop a mechanism to anonymize, ag-
13 gregate, and share the testing results from cyberse-
14 curity test beds to facilitate technology improve-
15 ments by public and private sector researchers.

16 “(b) BEST PRACTICES.—The Secretary, in collabora-
17 tion with the Director of the National Institute of Stand-
18 ards and Technology, the Director of the Cybersecurity
19 and Infrastructure Security Agency, and other appropriate
20 Federal agencies, shall convene relevant stakeholders and
21 facilitate the development of—

22 “(1) consensus-based best practices to improve
23 cybersecurity for—

24 “(A) emerging energy technologies;

1 “(B) distributed generation and storage
2 technologies, and other distributed energy re-
3 sources;

4 “(C) electric vehicles and electric vehicle
5 charging stations; and

6 “(D) other technologies and devices that
7 connect to the electric grid;

8 “(2) recommended cybersecurity designs and
9 technical requirements that can be used by the pri-
10 vate sector to design and build interoperable cyber-
11 security features into technologies that connect to
12 the electric grid, including networked devices and
13 components on distribution systems; and

14 “(3) technical analysis that can be used by the
15 private sector in developing best practices for test
16 beds and test bed methodologies that will enable re-
17 producible testing of cybersecurity protections for in-
18 formation systems, electronic devices, and other rel-
19 evant components, software, and hardware across
20 test beds.

21 “(c) REGULATORY AUTHORITY.—None of the activi-
22 ties authorized in this section shall be construed to author-
23 ize regulatory actions. Additionally, the voluntary stand-
24 ards developed under this section shall not duplicate or
25 conflict with mandatory reliability standards.

1 **“SEC. 8016. VULNERABILITY TESTING AND TECHNICAL AS-**
2 **SISTANCE TO IMPROVE CYBERSECURITY.**

3 “The Secretary shall—

4 “(1) coordinate with appropriate Federal agen-
5 cies and energy sector asset owners and operators,
6 leveraging the research facilities and expertise of the
7 National Laboratories, to assist entities in devel-
8 oping testing capabilities by—

9 “(A) utilizing a range of methods to iden-
10 tify vulnerabilities in physical and cyber sys-
11 tems;

12 “(B) developing cybersecurity risk assess-
13 ment tools and providing analyses and rec-
14 ommendations to participating stakeholders;
15 and

16 “(C) working with appropriate Federal
17 agencies and stakeholders to develop methods to
18 share anonymized and aggregated test results
19 to assist relevant stakeholders in the energy
20 sector, researchers, and the private sector to
21 advance cybersecurity efforts, technologies, and
22 tools;

23 “(2) collaborate with relevant stakeholders, in-
24 cluding public utility commissions, to—

25 “(A) identify information, research, staff
26 training, and analytical tools needed to evaluate

1 cybersecurity issues and challenges in the en-
2 ergy sector; and

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

6 “(3) coordinate with tribal governments to iden-
7 tify information, research, and analysis tools needed
8 by tribal governments to increase the cybersecurity
9 of energy assets within their jurisdiction.

10 **“SEC. 8017. CYBERSECURITY EDUCATION AND WORKFORCE**
11 **TRAINING RESEARCH AND STANDARDS.**

12 “(a) IN GENERAL.—The Secretary shall support the
13 development of a cybersecurity workforce through a pro-
14 gram that—

15 “(1) facilitates collaboration between under-
16 graduate and graduate students, researchers at the
17 National Laboratories, and the private sector;

18 “(2) prioritizes science and technology in areas
19 relevant to the mission of the Department of Energy
20 through the design and application of cybersecurity
21 technologies for the energy sector;

22 “(3) develops, or facilitates private sector devel-
23 opment of, voluntary cybersecurity training and re-
24 training standards, lessons, and recommendations

1 for the energy sector that minimize duplication of
2 cybersecurity compliance training programs; and

3 “(4) maintains a public database of energy sec-
4 tor cybersecurity education, training, and certifi-
5 cation programs.

6 “(b) GRID RESILIENCE TECHNOLOGY TRAINING.—
7 The Secretary shall support the development of the grid
8 workforce through a training program that prioritizes ac-
9 tivities that enhance the resilience of the electric grid and
10 energy sector infrastructure, including training on the use
11 of tools, technologies, and methods developed under the
12 grant program established in section 1311(b).

13 “(c) COLLABORATION.—In carrying out the program
14 authorized in subsection (a) and (b), the Secretary shall
15 coordinate with appropriate Federal agencies and leverage
16 programs and activities carried out across the Department
17 of Energy, other relevant Federal agencies, institutions of
18 higher education, and other appropriate entities best suit-
19 ed to provide national leadership on cybersecurity and grid
20 resilience-related issues.

1 **“SEC. 8018. INTERAGENCY COORDINATION AND STRATEGIC**
2 **PLAN FOR ENERGY SECTOR CYBERSECURITY**
3 **RESEARCH.**

4 “(a) DUTIES.—The Secretary, in coordination with
5 appropriate Federal agencies and the Energy Sector Gov-
6 ernment Coordinating Council, shall—

7 “(1) review the most recent versions of the
8 Roadmap to Achieve Energy Delivery Systems Cy-
9 bersecurity and the Multi-Year Program Plan for
10 Energy Sector Cybersecurity to identify crosscutting
11 energy sector cybersecurity research needs and op-
12 portunities for collaboration among Federal agencies
13 and other relevant stakeholders;

14 “(2) identify interdisciplinary research, tech-
15 nology, and tools that can be applied to cybersecu-
16 rity challenges in the energy sector;

17 “(3) identify technology transfer opportunities
18 to accelerate the development and commercial appli-
19 cation of novel cybersecurity technologies, systems,
20 and processes in the energy sector; and

21 “(4) develop a coordinated Interagency Stra-
22 tegic Plan for research to advance cybersecurity ca-
23 pabilities used in the energy sector that builds on
24 the Roadmap to Achieve Energy Delivery Systems in
25 Cybersecurity and the Multi-Year Program Plan for
26 Energy Sector Cybersecurity.

1 “(b) INTERAGENCY STRATEGIC PLAN.—

2 “(1) SUBMITTAL.—The Interagency Strategic
3 Plan developed under subsection (a)(4) shall be sub-
4 mitted to Congress and made public within 12
5 months after the date of enactment of the Grid Se-
6 curity Research and Development Act.

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

9 “(A) an analysis of how existing cybersecu-
10 rity research efforts across the Federal Govern-
11 ment are advancing the goals of the Roadmap
12 to Achieve Energy Delivery Systems Cybersecu-
13 rity and the Multi-Year Program Plan for En-
14 ergy Sector Cybersecurity;

15 “(B) recommendations for research areas
16 that may advance the cybersecurity of the en-
17 ergy sector;

18 “(C) an overview of existing and proposed
19 public and private sector research efforts that
20 address the topics outlined in paragraph (3);
21 and

22 “(D) an overview of needed support for
23 workforce training in cybersecurity for the en-
24 ergy sector.

1 “(3) CONSIDERATIONS.—In developing the
2 Interagency Strategic Plan, the Secretary, in coordi-
3 nation with appropriate Federal agencies and the
4 Energy Sector Government Coordinating Council,
5 shall consider—

6 “(A) opportunities for human factors re-
7 search to improve the design and effectiveness
8 of cybersecurity devices, technologies, tools,
9 processes, and training programs;

10 “(B) contributions of other disciplines to
11 the development of innovative cybersecurity pro-
12 cedures, devices, components, technologies, and
13 tools;

14 “(C) opportunities for technology transfer
15 programs to facilitate private sector develop-
16 ment of cybersecurity procedures, devices, com-
17 ponents, technologies, and tools for the energy
18 sector;

19 “(D) broader applications of the work done
20 by relevant Federal agencies to advance the cy-
21 bersecurity of information systems and data
22 analytics systems for the energy sector; and

23 “(E) activities called for in the Federal cy-
24 bersecurity research and development strategic
25 plan required by section 201(a)(1) of the Cy-

1 bersecurity Enhancement Act of 2014 (15
2 U.S.C. 7431(a)(1)).

3 “(c) PARTICIPATION.—For the purposes of carrying
4 out this section, the Energy Sector Government Coordi-
5 nating Council shall include representatives from Federal
6 agencies with expertise in the energy sector, information
7 systems, data analytics, cyber and physical systems, engi-
8 neering, human factors research, human-machine inter-
9 faces, high performance computing, big data and data
10 analytics, or other disciplines considered appropriate by
11 the Council Chair.

12 **“SEC. 8019. REPORT TO CONGRESS.**

13 “(a) STUDY.—The Secretary, in collaboration with
14 the National Institute of Standards and Technology, other
15 Federal agencies, and energy sector stakeholders, in order
16 to provide recommendations for additional research, devel-
17 opment, demonstration, and commercial application activi-
18 ties, shall—

19 “(1) analyze physical and cyber attacks on en-
20 ergy sector infrastructure and information systems
21 and identify cost-effective opportunities to improve
22 physical and cybersecurity; and

23 “(2) examine the risks associated with increas-
24 ing penetration of digital technologies in grid net-
25 works, particularly on the distribution grid.

1 “(b) CONTENT.—The study shall—

2 “(1) analyze processes, operational procedures,
3 and other factors common among cyber attacks;

4 “(2) identify areas where human behavior plays
5 a critical role in maintaining or compromising the
6 security of a system;

7 “(3) recommend—

8 “(A) changes to the design of devices,
9 human-machine interfaces, technologies, tools,
10 processes, or procedures to optimize security
11 that do not require a change in human behav-
12 ior; and

13 “(B) training techniques to increase the
14 capacity of employees to actively identify, pre-
15 vent, or neutralize the impact of cyber attacks;

16 “(4) evaluate existing engineering and technical
17 design criteria and guidelines that incorporate
18 human factors research findings, and recommend
19 criteria and guidelines for cybersecurity tools that
20 can be used to develop display systems for cyberse-
21 curity monitoring, such as alarms, user-friendly dis-
22 plays, and layouts;

23 “(5) evaluate the cybersecurity risks and bene-
24 fits of various design and architecture options for
25 energy sector systems, networked grid systems and

1 components, and automation systems, including con-
2 sideration of—

3 “(A) designs that include both digital and
4 analog control devices and technologies;

5 “(B) different communication technologies
6 used to transfer information and data between
7 control system devices, technologies, and system
8 operators;

9 “(C) automated and human-in-the-loop de-
10 vices and technologies;

11 “(D) programmable versus nonprogram-
12 mable devices and technologies;

13 “(E) increased redundancy using dissimilar
14 cybersecurity technologies; and

15 “(F) grid architectures that use autono-
16 mous functions to limit control vulnerabilities;
17 and

18 “(6) recommend methods or metrics to docu-
19 ment changes in risks associated with system de-
20 signs and architectures.

21 “(c) CONSULTATION.—In conducting the study, the
22 Secretary shall consult with energy sector stakeholders,
23 academic researchers, the private sector, and other rel-
24 evant stakeholders.

1 “(d) REPORT.—Not later than 24 months after the
 2 date of enactment of the Grid Security Research and De-
 3 velopment Act, the Secretary shall submit the study to the
 4 Committee on Science, Space, and Technology of the
 5 House of Representatives and the Committee on Energy
 6 and Natural Resources of the Senate.

7 **“SEC. 8020. CRITICAL INFRASTRUCTURE RESEARCH AND**
 8 **CONSTRUCTION.**

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

13 “(b) CRITICAL INFRASTRUCTURE DEFINED.—In this
 14 section, the term ‘critical infrastructure’ means infrastruc-
 15 ture that the Secretary determines to be vital to socio-
 16 economic activities such that, if destroyed or damaged,
 17 such destruction or damage could cause substantial dis-
 18 ruption to such socioeconomic activities.

19 “(c) COORDINATION.—In carrying out the program
 20 under subsection (a), the Secretary shall leverage expertise
 21 and resources of and facilitate collaboration and coordina-
 22 tion between—

23 “(1) relevant programs and activities across the
 24 Department;

25 “(2) the Department of Defense; and

1 “(3) the Department of Homeland Security.

2 “(d) ENERGY SECTOR CRITICAL INFRASTRUCTURE
3 TEST FACILITY.—In carrying out the program under sub-
4 section (a), the Secretary, in consultation with other ap-
5 propriate Federal agencies, shall establish and operate an
6 Energy Sector Critical Infrastructure Test Facility (re-
7 ferred to in this section as the ‘Test Facility’) that allows
8 for scalable physical and cyber performance testing to be
9 conducted on industry-scale energy sector critical infra-
10 structure systems. This facility shall include a focus on—

11 “(1) cybersecurity test beds; and

12 “(2) electric grid test beds.

13 “(e) SELECTION.—The Secretary shall select the
14 Test Facility under this section on a competitive, merit-
15 reviewed basis. The Secretary shall consider applications
16 from National Laboratories, institutions of higher edu-
17 cation, multi-institutional collaborations, and other appro-
18 priate entities.

19 “(f) DURATION.—The Test Facility established
20 under this section shall receive support for a period of not
21 more than 5 years, subject to the availability of appropria-
22 tions.

23 “(g) RENEWAL.—Upon the expiration of any period
24 of support of the Test Facility, the Secretary may renew

1 support for the Test Facility, on a merit-reviewed basis,
2 for a period of not more than 5 years.

3 “(h) TERMINATION.—Consistent with the existing
4 authorities of the Department, the Secretary may termi-
5 nate the Test Facility for cause during the performance
6 period.

7 **“SEC. 8021. DEFINITIONS.**

8 “In this title:

9 “(1) BIG DATA.—The term ‘big data’ means
10 datasets that require advanced analytical methods
11 for their transformation into useful information.

12 “(2) CYBERSECURITY.—The term ‘cybersecu-
13 rity’ means protecting an information system or in-
14 formation that is stored on, processed by, or
15 transiting an information system from a cybersecu-
16 rity threat or security vulnerability.

17 “(3) CYBERSECURITY THREAT.—The term ‘cy-
18 bersecurity threat’ has the meaning given the term
19 in section 102 of the Cybersecurity Information
20 Sharing Act of (6 U.S.C. 1501).

21 “(4) DEPARTMENT.—The term ‘Department’
22 means the Department Of Energy.

23 “(5) ELECTRICITY SUBSECTOR COORDINATING
24 COUNCIL.—The term ‘Electricity Subsector Coordi-
25 nating Council’ means the self-organized, self-gov-

1 erned council consisting of senior industry represent-
2 atives to serve as the principal liaison between the
3 Federal Government and the electric power sector
4 and to carry out the role of the Sector Coordinating
5 Council as established in the National Infrastructure
6 Protection Plan for the electricity subsector.

7 “(6) ENERGY SECTOR GOVERNMENT COORDI-
8 NATING COUNCIL.—The term ‘Energy Sector Gov-
9 ernment Coordinating Council’ means the council
10 consisting of representatives from relevant Federal
11 Government agencies to provide effective coordina-
12 tion of energy sector efforts to ensure a secure, reli-
13 able, and resilient energy infrastructure and to carry
14 out the role of the Government Coordinating Council
15 as established in the National Infrastructure Protec-
16 tion Plan for the energy sector.

17 “(7) HISTORICALLY BLACK COLLEGE OR UNI-
18 VERSITY.—The term ‘historically Black college or
19 university’ has the meaning given the term ‘part B
20 institution’ in section 322(2) of the Higher Edu-
21 cation Act of 1965 (29 U.S.C. 106(2)).

22 “(8) HUMAN FACTORS RESEARCH.—The term
23 ‘human factors research’ means research on human
24 performance in social and physical environments,
25 and on the integration and interaction of humans

1 with physical systems and computer hardware and
2 software.

3 “(9) HUMAN-MACHINE INTERFACES.—The term
4 ‘human-machine interfaces’ means technologies that
5 present information to an operator or user about the
6 state of a process or system, or accept human in-
7 structions to implement an action, including visual-
8 ization displays such as a graphical user interface.

9 “(10) INFORMATION SYSTEM.—The term ‘infor-
10 mation system’—

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

14 “(B) includes operational technology, infor-
15 mation technology, and communications.

16 “(11) MINORITY-SERVING INSTITUTION.—The
17 term ‘minority-serving institution’ means an eligible
18 institution under section 371(a) of the Higher Edu-
19 cation Act of 1965 (20 U.S.C. 1067q(a)).

20 “(12) NATIONAL LABORATORY.—The term ‘na-
21 tional laboratory’ has the meaning given the term in
22 section 2 of the Energy Policy Act of 2005 (42
23 U.S.C. 15801).

24 “(13) SECRETARY.—The term ‘Secretary’
25 means the Secretary of Energy.

1 “(14) SECURITY VULNERABILITY.—The term
2 ‘security vulnerability’ has the meaning given the
3 term in section 102 of the Cybersecurity Information
4 Sharing Act of 2015 (6 U.S.C. 1501).

5 “(15) TRANSIENT DEVICES.—The term ‘tran-
6 sient devices’ means removable media, including
7 floppy disks, compact disks, USB flash drives, exter-
8 nal hard drives, mobile devices, and other devices
9 that utilize wireless connections.”.

10 **SEC. 4. AUTHORIZATION OF APPROPRIATIONS.**

11 Section 8012 of division Z of the Consolidated Appro-
12 priations Act, 2021 (Public Law 116–260) is amended by
13 striking subsection (b)(1) and inserting the following:

14 “(1) to carry out sections 8006, 8013, 8014,
15 8015, 8016, 8017, 8018, 8019, 8020 and the
16 amendments made by sections 8001, 8002, and
17 8005 of this title—

18 “(A) \$371,000,000 for fiscal year 2022;

19 “(B) \$385,550,000 for fiscal year 2023;

20 “(C) \$400,577,500 for fiscal year 2024;

21 “(D) \$420,606,375 for fiscal year 2025;

22 and

23 “(E) \$441,636,694 for fiscal year 2026.”.

1 **SEC. 5. CONFORMING AMENDMENTS.**

2 (a) Section 101(b) of the division Z of the Consoli-
3 dated Appropriations Act, 2021 (Public Law 116–260) is
4 amended in the table of contents—

5 (1) in the matter relating to 8013, by striking
6 “8013” and inserting “8022”;

7 (2) in the matter relating to 8014, by striking
8 “8014” and inserting “8023”;

9 (3) in the matter relating to 8015, by striking
10 “8015” and inserting “8024”;

11 (4) by adding after the matter relating to sec-
12 tion 8012 the following:

“Sec. 8013. Energy sector security research, development, and demonstration
program.

“Sec. 8014. Grid resilience and emergency response.

“Sec. 8015. Best practices and guidance documents for energy sector cyberse-
curity research.

“Sec. 8016. Vulnerability testing and technical assistance to improve cyberse-
curity.

“Sec. 8017. Cybersecurity education and workforce training research and
standards.

“Sec. 8018. Interagency coordination and strategic plan for energy sector cy-
bersecurity research.

“Sec. 8019. Report to Congress.

“Sec. 8020. Critical infrastructure research and construction.

“Sec. 8021. Definitions.”.

13 (b) Sections 8013 through 8015 of division Z of the
14 Consolidated Appropriations Act, 2021 (Public Law 116–
15 260) are redesignated as sections 8022 through 8024, re-
16 spectively.

○