

116TH CONGRESS
2D SESSION

H. R. 5760

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 30 (legislative day, SEPTEMBER 29), 2020

Received; read twice and referred to the Committee on Energy and Natural
Resources

AN ACT

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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Grid Security Research
3 and Development Act”.

4 **SEC. 2. FINDINGS.**

5 Congress finds the following:

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

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

12 (3) The cybersecurity threat landscape is con-
13 stantly changing and attacker capabilities are ad-
14 vancing rapidly, requiring ongoing modifications, ad-
15 vancements, and investments in technologies and
16 procedures to maintain security.

17 (4) It is in the national interest for Federal
18 agencies to invest in cybersecurity research that in-
19 forms and facilitates private sector investment and
20 use of advanced cybersecurity tools and procedures
21 to protect information systems.

22 (5) The number of devices and systems con-
23 necting to the electric grid is increasing, and inte-
24 grating cybersecurity protections into information
25 systems when they are built is more effective than

1 modifying products after installation to meet
2 cybersecurity goals.

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

11 **SEC. 3. AMENDMENT TO ENERGY INDEPENDENCE AND SE-**
12 **CURITY ACT OF 2007.**

13 Title XIII of the Energy Independence and Security
14 Act of 2007 (42 U.S.C. 17381 et seq.) is amended by add-
15 ing at the end the following:

16 **“SEC. 1310. ENERGY SECTOR SECURITY RESEARCH, DEVEL-**
17 **OPMENT, AND DEMONSTRATION PROGRAM.**

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

1 cyber and physical attacks by increasing the cyber and
2 physical security capabilities of the energy sector and ac-
3 celerating the development of relevant technologies and
4 tools.

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

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

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

18 “(3) assess emerging cybersecurity capabilities
19 that could be applied to energy systems and develop
20 technologies that integrate cybersecurity features
21 and procedures into the design and development of
22 existing and emerging grid technologies, including
23 renewable energy, storage, and demand-side manage-
24 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
6 cybersecurity 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 that improve the
18 physical security of information systems, including
19 remote assets;

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

1 “(8) evaluate and understand the potential con-
2 sequences of practices used to maintain the
3 cybersecurity of information systems and intelligent
4 electronic 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 including electric grid and energy systems, including
2 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. 1311. 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 (c) on a competitive basis
18 to conduct research and development with the purpose of
19 improving the resilience and reliability of electric grid by—

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

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

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

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

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

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

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

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

6 “(c) ELIGIBLE ENTITIES.—The entities eligible to re-
7 ceive grants under this section include—

8 “(1) an institution of higher education;

9 “(2) a nonprofit organization;

10 “(3) a National Laboratory;

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

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

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

14 “(7) a private commercial entity;

15 “(8) a partnership or consortium of 2 or more
16 entities described in subparagraphs (1) through (7);
17 and

18 “(9) any other entities the Secretary deems ap-
19 propriate.

20 “(d) RELEVANT ACTIVITIES.—Grants awarded under
21 subsection (b) shall include funding for research and de-
22 velopment activities related to the purpose described in
23 subsection (b), such as—

24 “(1) development of technologies to use distrib-
25 uted energy resources, such as solar photovoltaics,

1 energy storage systems, electric vehicles, and
2 microgrids, to improve grid and critical end-user re-
3 silience;

4 “(2) analysis of non-technical barriers to great-
5 er integration and use of technologies on the dis-
6 tribution grid;

7 “(3) analysis of past large-area, long-duration
8 electricity interruptions to identify common elements
9 and best practices for electricity restoration, mitiga-
10 tion, and prevention of future disruptions;

11 “(4) development of advanced monitoring, ana-
12 lytics, operation, and controls of electric grid sys-
13 tems to improve electric grid resilience;

14 “(5) analysis of technologies, methods, and con-
15 cepts that can improve community resilience and
16 survivability of frequent or long-duration power out-
17 ages;

18 “(6) development of methodologies to maintain
19 cybersecurity during restoration of energy sector in-
20 frastructure and operation;

21 “(7) development of advanced power flow con-
22 trol systems and components to improve electric grid
23 resilience; and

24 “(8) any other relevant activities determined by
25 the Secretary.

1 “(e) TECHNICAL ASSISTANCE.—

2 “(1) IN GENERAL.—The Secretary shall provide
3 technical assistance to eligible entities for the com-
4 mercial application of technologies to improve the re-
5 silience of the electric grid and commercial applica-
6 tion of technologies to help entities develop plans for
7 preventing and recovering from various power out-
8 age scenarios at the local, regional, and State level.

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

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

19 “(B) the development of methods to
20 strengthen or otherwise mitigate adverse im-
21 pacts on electric grid infrastructure against
22 natural hazards;

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

1 “(D) a resource assessment and analysis of
2 future demand and distribution requirements,
3 including development of advanced grid archi-
4 tectures and risk analysis; and

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

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

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

22 “(3) ELIGIBLE ENTITIES.—The entities eligible
23 to receive technical assistance for commercial appli-
24 cation of technologies under this section include—

1 “(A) representatives of all sectors of the
2 electric power industry, including electric utili-
3 ties, trade organizations, and transmission and
4 distribution system organizations, owners, and
5 operators;

6 “(B) State and local governments and reg-
7 ulatory authorities, including public utility com-
8 missions;

9 “(C) tribal and Alaska Native govern-
10 mental entities;

11 “(D) partnerships among entities under
12 subparagraphs (A) through (C);

13 “(E) regional partnerships; and

14 “(F) any other entities the Secretary
15 deems appropriate.

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

20 **“SEC. 1312. BEST PRACTICES AND GUIDANCE DOCUMENTS**
21 **FOR ENERGY SECTOR CYBERSECURITY RE-**
22 **SEARCH.**

23 “(a) IN GENERAL.—The Secretary, in coordination
24 with appropriate Federal agencies, the Electricity Sub-
25 sector Coordinating Council, standards development orga-

1 nizations, State, tribal, local, and territorial governments,
2 the private sector, public utility commissions, and other
3 relevant stakeholders, shall coordinate the development of
4 guidance documents for research, development, and dem-
5 onstration activities to improve the cybersecurity capabili-
6 ties of the energy sector through participating agencies.
7 As part of these activities, the Secretary shall—

8 “(1) facilitate stakeholder involvement to up-
9 date—

10 “(A) the Roadmap to Achieve Energy De-
11 livery Systems Cybersecurity;

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

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

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

23 “(iii) managing supply chain risks;
24 and

1 “(C) the Electricity Subsector Cybersecu-
2 rity Capability Maturity Model, including the
3 development of metrics to measure changes in
4 cybersecurity readiness; and

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

7 “(A) developing standardized terminology
8 and monitoring processes; and

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

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

18 “(b) BEST PRACTICES.—The Secretary, in collabora-
19 tion with the Director of the National Institute of Stand-
20 ards and Technology and other appropriate Federal agen-
21 cies, shall convene relevant stakeholders and facilitate the
22 development of—

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

25 “(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. 1313. VULNERABILITY TESTING AND TECHNICAL AS-**
2 **SISTANCE TO IMPROVE CYBERSECURITY.**

3 “(a) IN GENERAL.—The Secretary shall—

4 “(1) coordinate with energy sector asset owners
5 and operators, leveraging the research facilities and
6 expertise of the National Laboratories, to assist enti-
7 ties in developing testing capabilities by—

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

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

15 “(C) working with stakeholders to develop
16 methods to share anonymized and aggregated
17 test results to assist relevant stakeholders in
18 the energy sector, researchers, and the private
19 sector to advance cybersecurity efforts, tech-
20 nologies, and tools;

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

23 “(A) identify information, research, staff
24 training, and analytical tools needed to evaluate
25 cybersecurity issues and challenges in the en-
26 ergy sector; and

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

4 “(3) collaborate with tribal governments to
5 identify information, research, and analysis tools
6 needed by tribal governments to increase the cyber-
7 security of energy assets within their jurisdiction.

8 **“SEC. 1314. EDUCATION AND WORKFORCE TRAINING RE-**
9 **SEARCH AND STANDARDS.**

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

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

16 “(2) prioritizes science and technology in areas
17 relevant to the mission of the Department of Energy
18 through the design and application of cybersecurity
19 technologies;

20 “(3) develops, or facilitates private sector devel-
21 opment of, voluntary cybersecurity training and re-
22 training standards, lessons, and recommendations
23 for the energy sector that minimize duplication of
24 cybersecurity compliance training programs; and

1 “(4) maintains a public database of
2 cybersecurity education, training, and certification
3 programs.

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

11 “(c) COLLABORATION.—In carrying out the program
12 authorized in subsection (a) and (b), the Secretary shall
13 leverage programs and activities carried out across the De-
14 partment of Energy, other relevant Federal agencies, in-
15 stitutions of higher education, and other appropriate enti-
16 ties best suited to provide national leadership on cyberse-
17 curity and grid resilience-related issues.

18 **“SEC. 1315. INTERAGENCY COORDINATION AND STRATEGIC**
19 **PLAN FOR ENERGY SECTOR CYBERSECURITY**
20 **RESEARCH.**

21 “(a) DUTIES.—The Secretary, in coordination with
22 the Energy Sector Government Coordinating Council,
23 shall—

24 “(1) review the most recent versions of the
25 Roadmap to Achieve Energy Delivery Systems

1 Cybersecurity and the Multi-Year Program Plan for
2 Energy Sector Cybersecurity to identify crosscutting
3 energy sector cybersecurity research needs and op-
4 portunities for collaboration among Federal agencies
5 and other relevant stakeholders;

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

9 “(3) identify technology transfer opportunities
10 to accelerate the development and commercial appli-
11 cation of novel cybersecurity technologies, systems,
12 and processes in the energy sector; and

13 “(4) develop a coordinated Interagency Stra-
14 tegic Plan for research to advance cybersecurity ca-
15 pabilities used in the energy sector that builds on
16 the Roadmap to Achieve Energy Delivery Systems in
17 Cybersecurity and the Multi-Year Program Plan for
18 Energy Sector Cybersecurity.

19 “(b) INTERAGENCY STRATEGIC PLAN.—

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

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

3 “(A) an analysis of how existing
4 cybersecurity research efforts across the Fed-
5 eral Government are advancing the goals of the
6 Roadmap to Achieve Energy Delivery Systems
7 Cybersecurity and the Multi-Year Program
8 Plan for Energy Sector Cybersecurity;

9 “(B) recommendations for research areas
10 that may advance the cybersecurity of the en-
11 ergy sector;

12 “(C) an overview of existing and proposed
13 public and private sector research efforts that
14 address the topics outlined in paragraph (3);
15 and

16 “(D) an overview of needed support for
17 workforce training in cybersecurity for the en-
18 ergy sector.

19 “(3) CONSIDERATIONS.—In developing the
20 Interagency Strategic Plan, the Secretary, in coordi-
21 nation with the Energy Sector Government Coordi-
22 nating Council, shall consider—

23 “(A) opportunities for human factors re-
24 search to improve the design and effectiveness

1 of cybersecurity devices, technologies, tools,
2 processes, and training programs;

3 “(B) contributions of other disciplines to
4 the development of innovative cybersecurity pro-
5 cedures, devices, components, technologies, and
6 tools;

7 “(C) opportunities for technology transfer
8 programs to facilitate private sector develop-
9 ment of cybersecurity procedures, devices, com-
10 ponents, technologies, and tools for the energy
11 sector;

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

16 “(E) activities called for in the Federal
17 cybersecurity research and development stra-
18 tegic plan required by section 201(a)(1) of the
19 Cybersecurity Enhancement Act of 2014 (15
20 U.S.C. 7431(a)(1)).

21 “(c) PARTICIPATION.—For the purposes of carrying
22 out this section, the Energy Sector Government Coordi-
23 nating Council shall include representatives from Federal
24 agencies with expertise in the energy sector, information
25 systems, data analytics, cyber and physical systems, engi-

1 neering, human factors research, human-machine inter-
2 faces, high performance computing, big data and data
3 analytics, or other disciplines considered appropriate by
4 the Council Chair.

5 **“SEC. 1316. REPORT TO CONGRESS.**

6 “(a) BALANCING RISKS, INCREASING SECURITY, AND
7 IMPROVING MODERNIZATION.—

8 “(1) STUDY.—The Secretary, in collaboration
9 with the National Institute of Standards and Tech-
10 nology, other Federal agencies, and energy sector
11 stakeholders, in order to provide recommendations
12 for additional research, development, demonstration,
13 and commercial application activities, shall—

14 “(A) analyze physical and cyber attacks on
15 energy sector infrastructure and information
16 systems and identify cost-effective opportunities
17 to improve physical and cyber security; and

18 “(B) examine the risks associated with in-
19 creasing penetration of digital technologies in
20 grid networks, particularly on the distribution
21 grid.

22 “(2) CONTENT.—The study shall—

23 “(A) analyze processes, operational proce-
24 dures, and other factors common among cyber
25 attacks;

1 “(B) identify areas where human behavior
2 plays a critical role in maintaining or compro-
3 mising the security of a system;

4 “(C) recommend—

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

10 “(ii) training techniques to increase
11 the capacity of employees to actively iden-
12 tify, prevent, or neutralize the impact of
13 cyber attacks;

14 “(D) evaluate existing engineering and
15 technical design criteria and guidelines that in-
16 corporate human factors research findings, and
17 recommend criteria and guidelines for cyberse-
18 curity tools that can be used to develop display
19 systems for cybersecurity monitoring, such as
20 alarms, user-friendly displays, and layouts;

21 “(E) evaluate the cybersecurity risks and
22 benefits of various design and architecture op-
23 tions for energy sector systems, networked grid
24 systems and components, and automation sys-
25 tems, including consideration of—

1 “(i) designs that include both digital
2 and analog control devices and tech-
3 nologies;

4 “(ii) different communication tech-
5 nologies used to transfer information and
6 data between control system devices, tech-
7 nologies, and system operators;

8 “(iii) automated and human-in-the-
9 loop devices and technologies;

10 “(iv) programmable versus non-
11 programmable devices and technologies;

12 “(v) increased redundancy using dis-
13 similar cybersecurity technologies; and

14 “(vi) grid architectures that use au-
15 tonomous functions to limit control
16 vulnerabilities; and

17 “(F) recommend methods or metrics to
18 document changes in risks associated with sys-
19 tem designs and architectures.

20 “(3) CONSULTATION.—In conducting the study,
21 the Secretary shall consult with energy sector stake-
22 holders, academic researchers, the private sector,
23 and other relevant stakeholders.

24 “(4) REPORT.—Not later than 24 months after
25 the date of enactment of the Grid Security Research

1 and Development Act, the Secretary shall submit the
2 study to the Committee on Science, Space, and
3 Technology of the House of Representatives and the
4 Committee on Energy and Natural Resources of the
5 Senate.

6 **“SEC. 1317. DEFINITIONS.**

7 “In this title:

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

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

16 “(3) CYBERSECURITY THREAT.—The term
17 ‘cybersecurity threat’ has the meaning given the
18 term in section 102 of the Cybersecurity Information
19 Sharing Act of 2015 (6 U.S.C. 1501).

20 “(4) ELECTRICITY SUBSECTOR COORDINATING
21 COUNCIL.—The term ‘Electricity Subsector Coordi-
22 nating Council’ means the self-organized, self-gov-
23 erned council consisting of senior industry represent-
24 atives to serve as the principal liaison between the
25 Federal Government and the electric power sector

1 and to carry out the role of the Sector Coordinating
2 Council as established in the National Infrastructure
3 Protection Plan for the electricity subsector.

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

14 “(6) HUMAN FACTORS RESEARCH.—The term
15 ‘human factors research’ means research on human
16 performance in social and physical environments,
17 and on the integration and interaction of humans
18 with physical systems and computer hardware and
19 software.

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

1 “(8) INFORMATION SYSTEM.—The term ‘infor-
2 mation system’—

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

6 “(B) includes operational technology, infor-
7 mation technology, and communications.

8 “(9) NATIONAL LABORATORY.—The term ‘na-
9 tional laboratory’ has the meaning given the term in
10 section 2 of the Energy Policy Act of 2005 (42
11 U.S.C. 15801).

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

16 “(11) TRANSIENT DEVICES.—The term ‘tran-
17 sient devices’ means removable media, including
18 floppy disks, compact disks, USB flash drives, exter-
19 nal hard drives, mobile devices, and other devices
20 that utilize wireless connections.

21 **“SEC. 1318. AUTHORIZATION OF APPROPRIATIONS.**

22 “‘There are authorized to be appropriated to the Sec-
23 retary to carry out this Act—

24 “(1) \$150,000,000 for fiscal year 2021;

25 “(2) \$157,500,000 for fiscal year 2022;

1 “(3) \$165,375,000 for fiscal year 2023;
2 “(4) \$173,645,000 for fiscal year 2024; and
3 “(5) \$182,325,000 for fiscal year 2025.”.

4 **SEC. 4. CRITICAL INFRASTRUCTURE RESEARCH AND CON-**
5 **STRUCTION.**

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

10 (b) CRITICAL INFRASTRUCTURE DEFINED.—The
11 term “critical infrastructure” means infrastructure that
12 the Secretary determines to be vital to socioeconomic ac-
13 tivities such that, if destroyed or damaged, such destruc-
14 tion or damage could cause substantial disruption to such
15 socioeconomic activities.

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

- 20 (1) relevant programs and activities across the
21 Department;
22 (2) the Department of Defense; and
23 (3) the Department of Homeland Security.

24 (d) CRITICAL INFRASTRUCTURE TEST FACILITY.—In
25 carrying out the program under subsection (a), the Sec-

1 retary shall establish and operate a Critical Infrastructure
2 Test Facility (referred to in this section as the “Test Fa-
3 cility”) that allows for scalable physical and cyber per-
4 formance testing to be conducted on industry-scale critical
5 infrastructure systems. This facility shall include a focus
6 on—

7 (1) cybersecurity test beds; and

8 (2) electric grid test beds.

9 (e) SELECTION.—The Secretary shall select the Test
10 Facility under this section on a competitive, merit-re-
11 viewed basis. The Secretary shall consider applications
12 from National Laboratories, institutions of higher edu-
13 cation, multi-institutional collaborations, and other appro-
14 priate entities.

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

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

22 (h) TERMINATION.—Consistent with the existing au-
23 thorities of the Department, the Secretary may terminate
24 the Test Facility for cause during the performance period.

1 **SEC. 5. CONFORMING AMENDMENT.**

2 Section 1(b) of the Energy Independence and Secu-
 3 rity Act of 2007 is amended in the table of contents by
 4 adding after the matter relating to section 1309 the fol-
 5 lowing:

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

“Sec. 1311. Grid resilience and emergency response.

“Sec. 1312. Best practices and guidance documents for energy sector cyberse-
 curity research.

“Sec. 1313. Vulnerability testing and technical assistance to improve cybersecu-
 rity.

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

“Sec. 1315. Interagency coordination and strategic plan for energy sector cy-
 bersecurity research.

“Sec. 1316. Report to Congress.

“Sec. 1317. Definitions.

“Sec. 1318. Authorization of appropriations.”.

Passed the House of Representatives September 29,
 2020.

Attest:

CHERYL L. JOHNSON,

Clerk.