

Union Calendar No. 391

116TH CONGRESS
2^D SESSION

H. R. 5760

[Report No. 116–489, Part I]

To provide for a comprehensive interdisciplinary research, development, and demonstration initiative to strengthen the capacity of the energy sector to prepare for and withstand cyber and physical attacks, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 5, 2020

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

SEPTEMBER 4, 2020

Reported from the Committee on Science, Space, and Technology with an amendment

[Strike out all after the enacting clause and insert the part printed in *italic*]

SEPTEMBER 4, 2020

Committee on Homeland Security discharged; committed to the Committee of the Whole House on the State of the Union and ordered to be printed

[For text of introduced bill, see copy of bill as introduced on February 5, 2020]

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”.*

6 **SEC. 2. FINDINGS.**

7 *Congress finds the following:*

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

10 *(2) Intelligent electronic devices, advanced ana-*
11 *lytics, and information systems used across the energy*
12 *sector are essential to maintaining reliable operation*
13 *of the electric grid.*

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

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

24 *(5) The number of devices and systems con-*
25 *necting to the electric grid is increasing, and inte-*

1 *grating cybersecurity protections into information*
2 *systems when they are built is more effective than*
3 *modifying products after installation to meet*
4 *cybersecurity goals.*

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

13 **SEC. 3. AMENDMENT TO ENERGY INDEPENDENCE AND SE-**
14 **CURITY ACT OF 2007.**

15 *Title XIII of the Energy Independence and Security*
16 *Act of 2007 (42 U.S.C. 17381 et seq.) is amended by adding*
17 *at the end the following:*

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

20 *“(a) IN GENERAL.—The Secretary, in coordination*
21 *with appropriate Federal agencies, the Electricity Subsector*
22 *Coordinating Council, the Electric Reliability Organiza-*
23 *tion, State, tribal, local, and territorial governments, the*
24 *private sector, and other relevant stakeholders, shall carry*
25 *out a research, development, and demonstration program*

1 *to protect the electric grid and energy systems, including*
2 *assets connected to the distribution grid, from cyber and*
3 *physical attacks by increasing the cyber and physical secu-*
4 *rity capabilities of the energy sector and accelerating the*
5 *development of relevant technologies and tools.*

6 “(b) *DEPARTMENT OF ENERGY.—As part of the initia-*
7 *tive described in subsection (a), the Secretary shall award*
8 *research, development, and demonstration grants 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 validate*
17 *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 and*
21 *procedures into the design and development of exist-*
22 *ing and emerging grid technologies, including renew-*
23 *able energy, storage, and demand-side management*
24 *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 management
11 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 stabi-
16 lizing 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, in-
23 cluding—

24 “(i) meters, phasor measurement units,
25 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 phys-*
18 *ical security of information systems, including remote*
19 *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 awareness;*

24 “(8) *evaluate and understand the potential con-*
25 *sequences of practices used to maintain the*

1 *cybersecurity of information systems and intelligent*
2 *electronic devices;*

3 “(9) *develop or expand the capabilities of exist-*
4 *ing cybersecurity test beds to simulate impacts of*
5 *cyber attacks and combined cyber-physical attacks on*
6 *information systems and electronic devices, including*
7 *by increasing access to existing and emerging test*
8 *beds for cooperative utilities, utilities owned by a po-*
9 *litical subdivision of a State, such as municipally-*
10 *owned electric utilities, and other relevant stake-*
11 *holders; and*

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

16 “(c) *NATIONAL SCIENCE FOUNDATION.—The National*
17 *Science Foundation, in coordination with other Federal*
18 *agencies as appropriate, shall through its cybersecurity re-*
19 *search and development programs—*

20 “(1) *support basic research to advance knowl-*
21 *edge, applications, technologies, and tools to strength-*
22 *en the cybersecurity of information systems, including*
23 *electric grid and energy systems, including inter-*
24 *disciplinary research in—*

1 “(A) *evolutionary systems, theories, mathe-*
2 *matics, and models;*

3 “(B) *economic and financial theories, math-*
4 *ematics, and models; and*

5 “(C) *big data analytical methods, mathe-*
6 *matics, computer coding, and algorithms; and*

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

13 “(d) *DEPARTMENT OF HOMELAND SECURITY SCIENCE*
14 *AND TECHNOLOGY DIRECTORATE.—The Science and Tech-*
15 *nology Directorate of the Department of Homeland Security*
16 *shall coordinate with the Department of Energy, the private*
17 *sector, and other relevant stakeholders, to research existing*
18 *cybersecurity technologies and tools used in the defense in-*
19 *dustry in order to—*

20 “(1) *identify technologies and tools that may*
21 *meet civilian energy sector cybersecurity needs;*

22 “(2) *develop a research strategy that incor-*
23 *porates human factors research findings to guide the*
24 *modification of defense industry cybersecurity tools*
25 *for use in the civilian sector;*

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

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

7 **“SEC. 1311. GRID RESILIENCE AND EMERGENCY RESPONSE.**

8 “(a) *IN GENERAL.—Not later than 180 days after the*
9 *enactment of the Grid Security Research and Development*
10 *Act, the Secretary shall establish a research, development,*
11 *and demonstration program to enhance resilience and*
12 *strengthen emergency response and management pertaining*
13 *to the energy sector.*

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

18 “(1) *developing methods to improve community*
19 *and governmental preparation for and emergency re-*
20 *sponse to large-area, long-duration electricity inter-*
21 *ruptions, including through the use of energy effi-*
22 *ciency, storage, and distributed generation tech-*
23 *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 be-
5 tween utilities and relevant Federal agencies to enable
6 communication, information-sharing, and situational
7 awareness in the event of a physical or cyber-attack
8 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 other
13 natural disasters;

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

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

23 “(7) upgrading tools used to estimate the costs of
24 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 devel-*
22 *opment activities related to the purpose described in sub-*
23 *section (b), such as—*

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

1 *ergy storage systems, electric vehicles, and microgrids,*
2 *to improve grid and critical end-user resilience;*

3 *“(2) analysis of non-technical barriers to greater*
4 *integration and use of technologies on the distribution*
5 *grid;*

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

10 *“(4) development of advanced monitoring, ana-*
11 *lytics, operation, and controls of electric grid systems*
12 *to improve electric grid resilience;*

13 *“(5) analysis of technologies, methods, and con-*
14 *cepts that can improve community resilience and sur-*
15 *vivability of frequent or long-duration power outages;*

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

19 *“(7) development of advanced power flow control*
20 *systems and components to improve electric grid resil-*
21 *ience; and*

22 *“(8) any other relevant activities determined by*
23 *the Secretary.*

24 *“(e) TECHNICAL ASSISTANCE.—*

1 “(1) *IN GENERAL.*—*The Secretary shall provide*
2 *technical assistance to eligible entities for the commer-*
3 *cial application of technologies to improve the resil-*
4 *ience of the electric grid and commercial application*
5 *of technologies to help entities develop plans for pre-*
6 *venting and recovering from various power outage*
7 *scenarios at the local, regional, and State level.*

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

12 “(A) *the commercial application of tech-*
13 *nologies developed from the grant program estab-*
14 *lished in subsection (b), including cooperative*
15 *utilities and utilities owned by a political sub-*
16 *division of a State, such as municipally-owned*
17 *electric utilities;*

18 “(B) *the development of methods to*
19 *strengthen or otherwise mitigate adverse impacts*
20 *on electric grid infrastructure against natural*
21 *hazards;*

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

24 “(D) *a resource assessment and analysis of*
25 *future demand and distribution requirements,*

1 *including development of advanced grid architec-*
2 *tures and risk analysis; and*

3 *“(E) the development of tools and tech-*
4 *nologies to coordinate data across relevant enti-*
5 *ties to promote resilience and wildfire prevention*
6 *in the planning, design, construction, operation,*
7 *and maintenance of transmission infrastructure;*

8 *“(F) analysis to predict the likelihood of ex-*
9 *treme weather events to inform the planning, de-*
10 *sign, construction, operation, and maintenance*
11 *of transmission infrastructure in consultation*
12 *with the National Oceanic and Atmospheric Ad-*
13 *ministration; and*

14 *“(G) the commercial application of relevant*
15 *technologies, such as distributed energy resources,*
16 *microgrids, or other energy technologies, to estab-*
17 *lish backup power for users or facilities affected*
18 *by emergency power shutoffs.*

19 *“(3) ELIGIBLE ENTITIES.—The entities eligible*
20 *to receive technical assistance for commercial applica-*
21 *tion of technologies under this section include—*

22 *“(A) representatives of all sectors of the elec-*
23 *tric power industry, including electric utilities,*
24 *trade organizations, and transmission and dis-*

1 *tribution system organizations, owners, and op-*
2 *erators;*

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

6 “(C) *tribal and Alaska Native governmental*
7 *entities;*

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

10 “(E) *regional partnerships; and*

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

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

17 **“SEC. 1312. 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 Subsector*
22 *Coordinating Council, standards development organiza-*
23 *tions, State, tribal, local, and territorial governments, the*
24 *private sector, public utility commissions, and other rel-*
25 *evant stakeholders, shall coordinate the development of guid-*

1 *ance documents for research, development, and demonstra-*
2 *tion activities to improve the cybersecurity capabilities of*
3 *the energy sector through participating agencies. As part*
4 *of these activities, the Secretary shall—*

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

7 *“(A) the Roadmap to Achieve Energy Deliv-*
8 *ery Systems Cybersecurity;*

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

12 *“(i) contracting with third parties to*
13 *conduct vulnerability testing for informa-*
14 *tion systems used across the energy produc-*
15 *tion, delivery, storage, and end use systems;*

16 *“(ii) contracting with third parties*
17 *that utilize transient devices to access infor-*
18 *mation systems; and*

19 *“(iii) managing supply chain risks;*
20 *and*

21 *“(C) the Electricity Subsector Cybersecurity*
22 *Capability Maturity Model, including the devel-*
23 *opment of metrics to measure changes in*
24 *cybersecurity readiness; and*

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

3 “(A) developing standardized terminology
4 and monitoring processes; and

5 “(B) utilizing human factors research to de-
6 velop more effective procedures for logging inci-
7 dent events; and

8 “(3) work with the National Science Foundation,
9 Department of Homeland Security, and stakeholders
10 to develop a mechanism to anonymize, aggregate, and
11 share the testing results from cybersecurity test beds
12 to facilitate technology improvements by public and
13 private sector researchers.

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

19 “(1) consensus-based best practices to improve
20 cybersecurity for—

21 “(A) emerging energy technologies;

22 “(B) distributed generation and storage
23 technologies, and other distributed energy re-
24 sources;

1 “(C) *electric vehicles and electric vehicle*
2 *charging stations; and*

3 “(D) *other technologies and devices that*
4 *connect to the electric grid;*

5 “(2) *recommended cybersecurity designs and*
6 *technical requirements that can be used by the private*
7 *sector to design and build interoperable cybersecurity*
8 *features into technologies that connect to the electric*
9 *grid, including networked devices and components on*
10 *distribution systems; and*

11 “(3) *technical analysis that can be used by the*
12 *private sector in developing best practices for test beds*
13 *and test bed methodologies that will enable reproduc-*
14 *ible testing of cybersecurity protections for informa-*
15 *tion systems, electronic devices, and other relevant*
16 *components, software, and hardware across test beds.*

17 “(c) *REGULATORY AUTHORITY.—None of the activities*
18 *authorized in this section shall be construed to authorize*
19 *regulatory actions. Additionally, the voluntary standards*
20 *developed under this section shall not duplicate or conflict*
21 *with mandatory reliability standards.*

22 “**SEC. 1313. VULNERABILITY TESTING AND TECHNICAL AS-**
23 **SISTANCE TO IMPROVE CYBERSECURITY.**

24 “(a) *IN GENERAL.—The Secretary shall—*

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

5 “(A) utilizing a range of methods to iden-
6 tify vulnerabilities in physical and cyber sys-
7 tems;

8 “(B) developing cybersecurity risk assess-
9 ment tools and providing analyses and rec-
10 ommendations to participating stakeholders; and

11 “(C) working with stakeholders to develop
12 methods to share anonymized and aggregated test
13 results to assist relevant stakeholders in the en-
14 ergy sector, researchers, and the private sector to
15 advance cybersecurity efforts, technologies, and
16 tools;

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

19 “(A) identify information, research, staff
20 training, and analytical tools needed to evaluate
21 cybersecurity issues and challenges in the energy
22 sector; and

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

1 “(3) collaborate with tribal governments to iden-
2 tify information, research, and analysis tools needed
3 by tribal governments to increase the cybersecurity of
4 energy assets within their jurisdiction.

5 **“SEC. 1314. EDUCATION AND WORKFORCE TRAINING RE-**
6 **SEARCH AND STANDARDS.**

7 “(a) *IN GENERAL.*—The Secretary shall support the
8 development of a cybersecurity workforce through a pro-
9 gram that—

10 “(1) facilitates collaboration between under-
11 graduate and graduate students, researchers at the
12 National Laboratories, and the private sector;

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

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

22 “(4) maintains a public database of
23 cybersecurity education, training, and certification
24 programs.

1 “(b) *GRID RESILIENCE TECHNOLOGY TRAINING.*—The
2 *Secretary shall support the development of the grid work-*
3 *force through a training program that prioritizes activities*
4 *that enhance the resilience of the electric grid and energy*
5 *sector infrastructure, including training on the use of tools,*
6 *technologies, and methods developed under the grant pro-*
7 *gram established in section 1311(b).*

8 “(c) *COLLABORATION.*—In carrying out the program
9 *authorized in subsection (a) and (b), the Secretary shall le-*
10 *verage programs and activities carried out across the De-*
11 *partment of Energy, other relevant Federal agencies, insti-*
12 *tutions of higher education, and other appropriate entities*
13 *best suited to provide national leadership on cybersecurity*
14 *and grid resilience-related issues.*

15 **“SEC. 1315. INTERAGENCY COORDINATION AND STRATEGIC**
16 **PLAN FOR ENERGY SECTOR CYBERSECURITY**
17 **RESEARCH.**

18 “(a) *DUTIES.*—The Secretary, in coordination with
19 *the Energy Sector Government Coordinating Council,*
20 *shall—*

21 “(1) *review the most recent versions of the Road-*
22 *map to Achieve Energy Delivery Systems*
23 *Cybersecurity and the Multi-Year Program Plan for*
24 *Energy Sector Cybersecurity to identify crosscutting*
25 *energy sector cybersecurity research needs and oppor-*

1 *tunities for collaboration among Federal agencies and*
2 *other relevant stakeholders;*

3 *“(2) identify interdisciplinary research, tech-*
4 *nology, and tools that can be applied to cybersecurity*
5 *challenges in the energy sector;*

6 *“(3) identify technology transfer opportunities to*
7 *accelerate the development and commercial applica-*
8 *tion of novel cybersecurity technologies, systems, and*
9 *processes in the energy sector; and*

10 *“(4) develop a coordinated Interagency Strategic*
11 *Plan for research to advance cybersecurity capabili-*
12 *ties used in the energy sector that builds on the Road-*
13 *map to Achieve Energy Delivery Systems in*
14 *Cybersecurity and the Multi-Year Program Plan for*
15 *Energy Sector Cybersecurity.*

16 *“(b) INTERAGENCY STRATEGIC PLAN.—*

17 *“(1) SUBMITTAL.—The Interagency Strategic*
18 *Plan developed under subsection (a)(4) shall be sub-*
19 *mitted to Congress and made public within 12*
20 *months after the date of enactment of the Grid Secu-*
21 *rity Research and Development Act.*

22 *“(2) CONTENTS.—The Interagency Strategic*
23 *Plan shall include—*

24 *“(A) an analysis of how existing*
25 *cybersecurity research efforts across the Federal*

1 *Government are advancing the goals of the Road-*
2 *map to Achieve Energy Delivery Systems*
3 *Cybersecurity and the Multi-Year Program Plan*
4 *for Energy Sector Cybersecurity;*

5 “(B) *recommendations for research areas*
6 *that may advance the cybersecurity of the energy*
7 *sector;*

8 “(C) *an overview of existing and proposed*
9 *public and private sector research efforts that ad-*
10 *dress the topics outlined in paragraph (3); and*

11 “(D) *an overview of needed support for*
12 *workforce training in cybersecurity for the en-*
13 *ergy sector.*

14 “(3) *CONSIDERATIONS.—In developing the Inter-*
15 *agency Strategic Plan, the Secretary, in coordination*
16 *with the Energy Sector Government Coordinating*
17 *Council, shall consider—*

18 “(A) *opportunities for human factors re-*
19 *search to improve the design and effectiveness of*
20 *cybersecurity devices, technologies, tools, proc-*
21 *esses, and training programs;*

22 “(B) *contributions of other disciplines to the*
23 *development of innovative cybersecurity proce-*
24 *dures, devices, components, technologies, and*
25 *tools;*

1 “(C) opportunities for technology transfer
2 programs to facilitate private sector development
3 of cybersecurity procedures, devices, components,
4 technologies, and tools for the energy sector;

5 “(D) broader applications of the work done
6 by relevant Federal agencies to advance the
7 cybersecurity of information systems and data
8 analytics systems for the energy sector; and

9 “(E) activities called for in the Federal
10 cybersecurity research and development strategic
11 plan required by section 201(a)(1) of the
12 Cybersecurity Enhancement Act of 2014 (15
13 U.S.C. 7431(a)(1)).

14 “(c) *PARTICIPATION.*—For the purposes of carrying
15 out this section, the Energy Sector Government Coordi-
16 nating Council shall include representatives from Federal
17 agencies with expertise in the energy sector, information
18 systems, data analytics, cyber and physical systems, engi-
19 neering, human factors research, human-machine inter-
20 faces, high performance computing, big data and data ana-
21 lytics, or other disciplines considered appropriate by the
22 Council Chair.

23 **“SEC. 1316. REPORT TO CONGRESS.**

24 “(a) *BALANCING RISKS, INCREASING SECURITY, AND*
25 *IMPROVING MODERNIZATION.*—

1 “(1) *STUDY.*—*The Secretary, in collaboration*
2 *with the National Institute of Standards and Tech-*
3 *nology, other Federal agencies, and energy sector*
4 *stakeholders, in order to provide recommendations for*
5 *additional research, development, demonstration, and*
6 *commercial application activities, shall—*

7 “(A) *analyze physical and cyber attacks on*
8 *energy sector infrastructure and information sys-*
9 *tems and identify cost-effective opportunities to*
10 *improve physical and cyber security; and*

11 “(B) *examine the risks associated with in-*
12 *creasing penetration of digital technologies in*
13 *grid networks, particularly on the distribution*
14 *grid.*

15 “(2) *CONTENT.*—*The study shall—*

16 “(A) *analyze processes, operational proce-*
17 *dures, and other factors common among cyber*
18 *attacks;*

19 “(B) *identify areas where human behavior*
20 *plays a critical role in maintaining or compro-*
21 *miting the security of a system;*

22 “(C) *recommend—*

23 “(i) *changes to the design of devices,*
24 *human-machine interfaces, technologies,*
25 *tools, processes, or procedures to optimize*

1 security that do not require a change in
2 human behavior; and

3 “(ii) training techniques to increase
4 the capacity of employees to actively iden-
5 tify, prevent, or neutralize the impact of
6 cyber attacks;

7 “(D) evaluate existing engineering and tech-
8 nical design criteria and guidelines that incor-
9 porate human factors research findings, and rec-
10 ommend criteria and guidelines for cybersecurity
11 tools that can be used to develop display systems
12 for cybersecurity monitoring, such as alarms,
13 user-friendly displays, and layouts;

14 “(E) evaluate the cybersecurity risks and
15 benefits of various design and architecture op-
16 tions for energy sector systems, networked grid
17 systems and components, and automation sys-
18 tems, including consideration of—

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

21 “(ii) different communication tech-
22 nologies used to transfer information and
23 data between control system devices, tech-
24 nologies, and system operators;

1 “(iii) automated and human-in-the-
2 loop devices and technologies;

3 “(iv) programmable versus non-
4 programmable devices and technologies;

5 “(v) increased redundancy using dis-
6 similar cybersecurity technologies; and

7 “(vi) grid architectures that use auton-
8 omous functions to limit control
9 vulnerabilities; and

10 “(F) recommend methods or metrics to doc-
11 ument changes in risks associated with system
12 designs and architectures.

13 “(3) CONSULTATION.—In conducting the study,
14 the Secretary shall consult with energy sector stake-
15 holders, academic researchers, the private sector, and
16 other relevant stakeholders.

17 “(4) REPORT.—Not later than 24 months after
18 the date of enactment of the Grid Security Research
19 and Development Act, the Secretary shall submit the
20 study to the Committee on Science, Space, and Tech-
21 nology of the House of Representatives and the Com-
22 mittee on Energy and Natural Resources of the Sen-
23 ate.

24 **“SEC. 1317. DEFINITIONS.**

25 *“In this title:*

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

4 “(2) *CYBERSECURITY*.—The term ‘cybersecurity’
5 *means protecting an information system or informa-*
6 *tion that is stored on, processed by, or transiting an*
7 *information system from a cybersecurity threat or se-*
8 *curity vulnerability.*

9 “(3) *CYBERSECURITY THREAT*.—The term
10 ‘*cybersecurity threat*’ has the meaning given the term
11 *in section 102 of the Cybersecurity Information Shar-*
12 *ing Act of 2015 (6 U.S.C. 1501).*

13 “(4) *ELECTRICITY SUBSECTOR COORDINATING*
14 *COUNCIL*.—The term ‘*Electricity Subsector Coordi-*
15 *nating Council*’ means the self-organized, self-gov-
16 *erned council consisting of senior industry representa-*
17 *tives to serve as the principal liaison between the Fed-*
18 *eral Government and the electric power sector and to*
19 *carry out the role of the Sector Coordinating Council*
20 *as established in the National Infrastructure Protec-*
21 *tion Plan for the electricity subsector.*

22 “(5) *ENERGY SECTOR GOVERNMENT COORDI-*
23 *NATING COUNCIL*.—The term ‘*Energy Sector Govern-*
24 *ment Coordinating Council*’ means the council con-
25 *sisting of representatives from relevant Federal Gov-*

1 *ernment agencies to provide effective coordination of*
2 *energy sector efforts to ensure a secure, reliable, and*
3 *resilient energy infrastructure and to carry out the*
4 *role of the Government Coordinating Council as estab-*
5 *lished in the National Infrastructure Protection Plan*
6 *for the energy sector.*

7 “(6) *HUMAN FACTORS RESEARCH.*—*The term*
8 *‘human factors research’ means research on human*
9 *performance in social and physical environments,*
10 *and on the integration and interaction of humans*
11 *with physical systems and computer hardware and*
12 *software.*

13 “(7) *HUMAN-MACHINE INTERFACES.*—*The term*
14 *‘human-machine interfaces’ means technologies that*
15 *present information to an operator or user about the*
16 *state of a process or system, or accept human instruc-*
17 *tions to implement an action, including visualization*
18 *displays such as a graphical user interface.*

19 “(8) *INFORMATION SYSTEM.*—*The term ‘informa-*
20 *tion system’—*

21 “(A) *has the meaning given the term in sec-*
22 *tion 102 of the Cybersecurity Information Shar-*
23 *ing Act of 2015 (6 U.S.C. 1501); and*

24 “(B) *includes operational technology, infor-*
25 *mation technology, and communications.*

1 “(9) *NATIONAL LABORATORY*.—*The term ‘na-*
2 *tional laboratory’ has the meaning given the term in*
3 *section 2 of the Energy Policy Act of 2005 (42 U.S.C.*
4 *15801).*

5 “(10) *SECURITY VULNERABILITY*.—*The term ‘se-*
6 *curity vulnerability’ has the meaning given the term*
7 *in section 102 of the Cybersecurity Information Shar-*
8 *ing Act of 2015 (6 U.S.C. 1501).*

9 “(11) *TRANSIENT DEVICES*.—*The term ‘transient*
10 *devices’ means removable media, including floppy*
11 *disks, compact disks, USB flash drives, external hard*
12 *drives, mobile devices, and other devices that utilize*
13 *wireless connections.*

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

15 *“There are authorized to be appropriated to the Sec-*
16 *retary to carry out this Act—*

17 “(1) \$150,000,000 for fiscal year 2021;

18 “(2) \$157,500,000 for fiscal year 2022;

19 “(3) \$165,375,000 for fiscal year 2023;

20 “(4) \$173,645,000 for fiscal year 2024; and

21 “(5) \$182,325,000 for fiscal year 2025.”.

22 **SEC. 4. CRITICAL INFRASTRUCTURE RESEARCH AND CON-**
23 **STRUCTION.**

24 *(a) IN GENERAL*.—*The Secretary shall carry out a*
25 *program of research, development, and demonstration of*

1 *technologies and tools to help ensure the resilience and secu-*
2 *rity of critical integrated grid infrastructures.*

3 (b) *CRITICAL INFRASTRUCTURE DEFINED.*—*The term*
4 *“critical infrastructure” means infrastructure that the Sec-*
5 *retary determines to be vital to socioeconomic activities*
6 *such that, if destroyed or damaged, such destruction or*
7 *damage could cause substantial disruption to such socio-*
8 *economic activities.*

9 (c) *COORDINATION.*—*In carrying out the program*
10 *under subsection (a), the Secretary shall leverage expertise*
11 *and resources of and facilitate collaboration and coordina-*
12 *tion between—*

13 (1) *relevant programs and activities across the*
14 *Department;*

15 (2) *the Department of Defense; and*

16 (3) *the Department of Homeland Security.*

17 (d) *CRITICAL INFRASTRUCTURE TEST FACILITY.*—*In*
18 *carrying out the program under subsection (a), the Sec-*
19 *retary shall establish and operate a Critical Infrastructure*
20 *Test Facility (referred to in this section as the “Test Facil-*
21 *ity”) that allows for scalable physical and cyber perform-*
22 *ance testing to be conducted on industry-scale critical infra-*
23 *structure systems. This facility shall include a focus on—*

24 (1) *cybersecurity test beds; and*

25 (2) *electric grid test beds.*

1 (e) *SELECTION.*—*The Secretary shall select the Test*
 2 *Facility under this section on a competitive, merit-reviewed*
 3 *basis. The Secretary shall consider applications from Na-*
 4 *tional Laboratories, institutions of higher education, multi-*
 5 *institutional collaborations, and other appropriate entities.*

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

9 (g) *RENEWAL.*—*Upon the expiration of any period of*
 10 *support of the Test Facility, the Secretary may renew sup-*
 11 *port for the Test Facility, on a merit-reviewed basis, for*
 12 *a period of not more than 5 years.*

13 (h) *TERMINATION.*—*Consistent with the existing au-*
 14 *thorities of the Department, the Secretary may terminate*
 15 *the Test Facility for cause during the performance period.*

16 **SEC. 5. CONFORMING AMENDMENT.**

17 *Section 1(b) of the Energy Independence and Security*
 18 *Act of 2007 is amended in the table of contents by adding*
 19 *after the matter relating to section 1309 the following:*

“Sec. 1310. *Energy sector security research, development, and demonstration pro-*
gram.”

“Sec. 1311. *Grid resilience and emergency response.*”

“Sec. 1312. *Best practices and guidance documents for energy sector cybersecurity*
research.”

“Sec. 1313. *Vulnerability testing and technical assistance to improve*
cybersecurity.”

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

“Sec. 1315. *Interagency coordination and strategic plan for energy sector*
cybersecurity research.”

“Sec. 1316. *Report to Congress.*”

“Sec. 1317. *Definitions.*”

“Sec. 1318. *Authorization of appropriations.*”.

Union Calendar No. 391

116TH CONGRESS
2^D SESSION

H. R. 5760

[Report No. 116-489, Part I]

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.

SEPTEMBER 4, 2020

Reported from the Committee on Science, Space, and
Technology with an amendment

SEPTEMBER 4, 2020

Committee on Homeland Security discharged; committed
to the Committee of the Whole House on the State of
the Union and ordered to be printed