

.....
(Original Signature of Member)

116TH CONGRESS
1ST SESSION

H. R. 5760

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

Mr. Bera (for himself and Mr. Weber) introduced the following bill; which was referred to the Committee on _____

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 and
13 procedures to maintain security.

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

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

25 (7) An understanding of human factors can be
26 leveraged to understand the behavior of cyber threat

1 actors, develop strategies to counter threat actors,
2 improve cybersecurity training programs, optimize
3 the design of human-machine interfaces and cyberse-
4 curity tools, and increase the capacity of the energy
5 sector workforce to prevent unauthorized access to
6 critical systems.

7 **SEC. 3. AMENDMENT TO ENERGY INDEPENDENCE AND SE-**
8 **CURITY ACT OF 2007.**

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

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

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

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

5 “(1) identify cybersecurity risks to information
6 systems within, and impacting, the electricity sector,
7 energy systems, and energy infrastructure;

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

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

21 “(4) identify existing vulnerabilities in intel-
22 ligent electronic devices, advanced analytics systems,
23 and information systems;

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

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

9 “(B) data storage systems, data manage-
10 ment systems, and data analysis processes;

11 “(C) automated- and manually-controlled
12 devices and equipment for monitoring and sta-
13 bilizing the electric grid;

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

18 “(E) power system delivery and end user
19 systems and devices that connect to the grid,
20 including—

21 “(i) meters, synchrophasors, phasor
22 measurement units, and other sensors;

23 “(ii) distribution automation tech-
24 nologies, smart inverters, and other grid
25 control technologies;

1 “(iii) distributed generation, energy
2 storage, and other distributed energy tech-
3 nologies;

4 “(iv) demand response technologies;

5 “(v) home and building energy man-
6 agement and control systems;

7 “(vi) electric and plug-in hybrid vehi-
8 cles and electric vehicle charging systems;
9 and

10 “(vii) other relevant devices, software,
11 firmware, and hardware; and

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

14 “(6) develop technologies that improve the
15 physical security of information systems, including
16 remote assets;

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

22 “(8) evaluate and understand the potential con-
23 sequences of practices used to maintain the cyberse-
24 curity of information systems and intelligent elec-
25 tronic devices;

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

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

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

18 “(1) support basic research to advance knowl-
19 edge, applications, technologies, and tools to
20 strengthen the cybersecurity of information systems,
21 including electric grid and energy systems, including
22 interdisciplinary research in—

23 “(A) evolutionary systems, theories, mathe-
24 matics, and models;

1 “(B) economic and financial theories,
2 mathematics, and models; and

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

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

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

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

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

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

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

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

8 “(a) IN GENERAL.—Not later than 180 days after
9 the enactment of the Grid Security Research and Develop-
10 ment Act, the Secretary shall establish a research, devel-
11 opment, and demonstration program to enhance resilience
12 and strengthen emergency response and management per-
13 taining 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
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 deteriorating electrical equipment on the
16 transmission and distribution grid, including detec-
17 tion of spark ignition causing wildfires and risks of
18 vegetation contact; and

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.

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

25 “(1) an institution of higher education;

1 “(2) a nonprofit organization;

2 “(3) a National Laboratory;

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

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

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

6 “(7) a private commercial entity;

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

9 and

10 “(9) any other entities the Secretary deems ap-
11 propriate.

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

16 “(1) development of technologies to use distrib-
17 uted energy resources, such as solar photovoltaics,
18 energy storage systems, electric vehicles, and
19 microgrids, to improve grid and critical end-user re-
20 silience;

21 “(2) analysis of non-technical barriers to great-
22 er integration and use of technologies on the dis-
23 tribution grid;

24 “(3) analysis of past large-area, long-duration
25 electricity interruptions to identify common elements

1 and best practices for electricity restoration, mitiga-
2 tion, and prevention of future disruptions;

3 “(4) development of advanced monitoring, ana-
4 lytics, operation, and controls of electricity grid sys-
5 tems to improve electric grid resilience;

6 “(5) analysis of technologies, methods, and con-
7 cepts that can improve community resilience and
8 survivability of frequent or long-duration power out-
9 ages;

10 “(6) development of methodologies to maintain
11 cybersecurity during restoration of energy sector in-
12 frastructure and operation;

13 “(7) development of advanced power flow con-
14 trol systems and components to improve electric grid
15 resilience; and

16 “(8) any other relevant activities determined by
17 the Secretary.

18 “(e) TECHNICAL ASSISTANCE.—

19 “(1) IN GENERAL.—The Secretary shall provide
20 technical assistance to eligible entities for the com-
21 mercial application of technologies to improve the re-
22 siliance of the electric grid and commercial applica-
23 tion of technologies to help entities develop plans for
24 preventing and recovering from various power out-
25 age scenarios at the local, regional, and State level.

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

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

11 “(B) the development of methods to
12 strengthen or otherwise mitigate adverse im-
13 pacts on electric grid infrastructure against
14 natural hazards;

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

17 “(D) a resource assessment and analysis of
18 future demand and distribution requirements,
19 including development of advanced grid archi-
20 tectures and risk analysis.

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

24 “(A) representatives of all sectors of the
25 electric power industry, including electric utili-

1 ties, trade organizations, and transmission and
2 distribution system organizations, owners, and
3 operators;

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

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

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

11 “(E) regional partnerships; and

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

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

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

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

1 relevant stakeholders, shall coordinate the development of
2 guidance documents for research, development, and dem-
3 onstration activities to improve the cybersecurity capabili-
4 ties of the energy sector through participating agencies.
5 As part of these activities, the Secretary 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 analyses 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 “(c) BEST PRACTICES.—The Secretary, in collabora-
17 tion with the Director of the National Institute of Stand-
18 ards and Technology and other appropriate Federal agen-
19 cies, shall convene relevant stakeholders and facilitate the
20 development of—

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

23 “(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 features and
9 requirements that can be used by the private sector
10 to design and build interoperable cybersecurity fea-
11 tures into technologies that connect to the electric
12 grid, including networked devices and components
13 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 “(d) 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 cybersecu-
2 rity education, training, and certification programs.

3 “(b) COLLABORATION.—In carrying out the program
4 authorized in subsection (a), the Secretary shall leverage
5 programs and activities carried out across the Department
6 of Energy, other relevant Federal agencies, institutions of
7 higher education, and other appropriate entities best suit-
8 ed to provide national leadership on cybersecurity-related
9 issues.

10 **“SEC. 1315. INTERAGENCY COORDINATION AND STRATEGIC**
11 **PLAN FOR ENERGY SECTOR CYBERSECURITY**
12 **RESEARCH.**

13 “(a) DUTIES.—The Secretary, in coordination with
14 the Energy Sector Government Coordinating Council,
15 shall—

16 “(1) review the most recent versions of the
17 Roadmap to Achieve Energy Delivery Systems Cy-
18 bersecurity and the Multi-Year Program Plan for
19 Energy Sector Cybersecurity to identify crosscutting
20 energy sector cybersecurity research needs and op-
21 portunities for collaboration among Federal agencies
22 and other relevant stakeholders;

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

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

5 “(4) develop a coordinated Interagency Stra-
6 tegic Plan for research to advance cybersecurity ca-
7 pabilities used in the energy sector that builds on
8 the Roadmap to Achieve Energy Delivery Systems in
9 Cybersecurity and the Multi-Year Program Plan for
10 Energy Sector Cybersecurity.

11 “(b) INTERAGENCY STRATEGIC PLAN.—

12 “(1) SUBMITTAL.—The Interagency Strategic
13 Plan developed under subsection (a)(4) shall be sub-
14 mitted to Congress within 12 months after the date
15 of enactment of the Grid Security Research and De-
16 velopment Act.

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

19 “(A) an analysis of how existing cybersecu-
20 rity research efforts across the Federal Govern-
21 ment are advancing the goals of the Roadmap
22 to Achieve Energy Delivery Systems Cybersecu-
23 rity and the Multi-Year Program Plan for En-
24 ergy Sector Cybersecurity;

1 “(B) recommendations for research areas
2 that may advance the cybersecurity of the en-
3 ergy sector;

4 “(C) an overview of existing and proposed
5 public and private sector research efforts that
6 address the topics outlined in paragraph (3);
7 and

8 “(D) an overview of needed support for
9 workforce training in cybersecurity for the en-
10 ergy sector.

11 “(3) CONSIDERATIONS.—In developing the
12 Interagency Strategic Plan, the Secretary, in coordi-
13 nation with the Energy Sector Government Coordi-
14 nating Council, shall consider—

15 “(A) opportunities for human factors re-
16 search to improve the design and effectiveness
17 of cybersecurity devices, technologies, tools,
18 processes, and training programs;

19 “(B) contributions of other disciplines to
20 the development of innovative cybersecurity pro-
21 cedures, devices, components, technologies, and
22 tools;

23 “(C) opportunities for technology transfer
24 programs to facilitate private sector develop-
25 ment of cybersecurity procedures, devices, com-

1 ponents, technologies, and tools for the energy
2 sector;

3 “(D) broader applications of the work done
4 by relevant Federal agencies to advance the cy-
5 bersecurity of information systems and data
6 analytics systems for the energy sector; and

7 “(E) activities called for in the Federal cy-
8 bersecurity research and development strategic
9 plan required by section 201(a)(1) of the Cy-
10 bersecurity Enhancement Act of 2014 (15
11 U.S.C. 7431(a)(1)).

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

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

22 “(a) BALANCING RISKS, INCREASING SECURITY, AND
23 IMPROVING MODERNIZATION.—

24 “(1) STUDY.—The Secretary, in collaboration
25 with the National Institute of Standards and Tech-

1 nology, other Federal agencies, and energy sector
2 stakeholders, in order to provide recommendations
3 for additional research, development, demonstration,
4 and commercial application activities, shall—

5 “(A) analyze physical and cyber attacks on
6 energy sector infrastructure and information
7 systems and identify cost-effective opportunities
8 to improve physical and cyber security; and

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

13 “(2) CONTENT.—The study shall—

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

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

20 “(C) recommend—

21 “(i) changes to the design of devices,
22 human-machine interfaces, technologies,
23 tools, processes, or procedures to optimize
24 security that do not require a change in
25 human behavior; and

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

5 “(D) evaluate existing engineering and
6 technical design criteria and guidelines that in-
7 corporate human factors research findings, and
8 recommend criteria and guidelines for cyberse-
9 curity tools that can be used to develop display
10 systems for cybersecurity monitoring, such as
11 alarms, user-friendly displays, and layouts;

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

17 “(i) designs that include both digital
18 and analog control devices and tech-
19 nologies;

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

24 “(iii) automated and human-in-the-
25 loop devices and technologies;

1 “(iv) programmable versus non-
2 programmable devices and technologies;

3 “(v) increased redundancy using dis-
4 similar cybersecurity technologies; and

5 “(vi) grid architectures that use au-
6 tonomous functions to limit control
7 vulnerabilities; and

8 “(F) recommend methods or metrics to
9 document changes in risks associated with sys-
10 tem designs and architectures.

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

15 “(4) REPORT.—Not later than 24 months after
16 the date of enactment of the Grid Security Research
17 and Development Act, the Secretary shall submit the
18 study to the Committee on Science, Space, and
19 Technology of the House of Representatives and the
20 Committee on Energy and Natural Resources of the
21 Senate.

22 **“SEC. 1317. DEFINITIONS.**

23 “‘In this title:

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

4 “(2) CYBERSECURITY.—The term ‘cybersecu-
5 rity’ means protecting an information system or in-
6 formation that is stored on, processed by, or
7 transiting an information system from a cybersecu-
8 rity threat or security vulnerability.

9 “(3) CYBERSECURITY THREAT.—The term ‘cy-
10 bersecurity threat’ has the meaning given the term
11 in section 102 of the Cybersecurity Information
12 Sharing 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 represent-
17 atives to serve as the principal liaison between the
18 Federal Government and the electric power sector
19 and to carry out the role of the Sector Coordinating
20 Council as established in the National Infrastructure
21 Protection Plan for the electricity subsector.

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

1 Government agencies to provide effective coordina-
2 tion of energy sector efforts to ensure a secure, reli-
3 able, and resilient energy infrastructure and to carry
4 out the role of the Government Coordinating Council
5 as established in the National Infrastructure Protec-
6 tion Plan 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 in-
17 structions to implement an action, including visual-
18 ization displays such as a graphical user interface.

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

21 “(A) has the meaning given the term in
22 section 102 of the Cybersecurity Information
23 Sharing 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
4 U.S.C. 15801).

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

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

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

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

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.”.