

114TH CONGRESS
2D SESSION

H. R. 6227

To provide for a comprehensive interdisciplinary research and development initiative to strengthen the capacity of the electricity sector to neutralize cyber attacks.

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 28, 2016

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

A BILL

To provide for a comprehensive interdisciplinary research and development initiative to strengthen the capacity of the electricity sector to neutralize cyber attacks.

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 Cybersecurity Re-
5 search and Development Act”.

6 **SEC. 2. FINDINGS.**

7 Congress finds the following:

1 (1) The Nation, and every other critical infra-
2 structure sector, depends on reliable electricity.

3 (2) Industrial control systems used in the elec-
4 tricity sector are essential to maintain reliable oper-
5 ations of the electric grid.

6 (3) The cybersecurity threat landscape is con-
7 stantly changing and attacker capabilities are ad-
8 vancing rapidly, requiring ongoing modifications, ad-
9 vancements, and investments in technologies and
10 procedures to maintain security.

11 (4) There are substantial and important dif-
12 ferences between cybersecurity approaches needed to
13 protect information technology systems and indus-
14 trial control systems.

15 (5) It is in the national interest for Federal
16 agencies to invest in industrial control system cyber-
17 security research that facilitates private sector in-
18 vestment and the ability of the private sector to de-
19 velop cybersecurity tools and products for control
20 systems.

21 (6) The number of elements connecting to the
22 electric grid is increasing, and designing cybersecu-
23 rity into communication, data, and control systems
24 when they are built is more effective than modifying

1 products after installation to meet cybersecurity
2 goals.

3 (7) 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 industrial control system cybersecurity
7 training programs, optimize the design of human-
8 machine interfaces and cybersecurity tools, and in-
9 crease the capacity of the electrical sector workforce
10 to prevent attacks from gaining entry to industrial
11 control systems.

12 **SEC. 3. DEFINITIONS.**

13 In this Act:

14 (1) CRITICAL ELECTRIC INFRASTRUCTURE IN-
15 FORMATION.—The term “critical electric infrastruc-
16 ture information” has the meaning given that term
17 in section 215A(a)(3) of the Federal Power Act (16
18 U.S.C. 824a–1(a)(3)).

19 (2) CYBERSECURITY.—The term “cyber-
20 security” means a set of preventative measures to
21 protect information from a digital device or system,
22 including a device or system used to manage the
23 electric grid, from being stolen, compromised, or
24 used to carry out an attack.

1 (3) ELECTRICITY SUBSECTOR COORDINATING
2 COUNCIL.—The term “Electricity Subsector Coordinating Council” means the self-organized, self-governed council consisting of senior industry representatives to serve as the principal liaison between the Federal Government and the electric power sector and to carry out the role of the Sector Coordinating Council as established in the National Infrastructure Protection Plan for the electricity subsector.

10 (4) ENERGY SECTOR GOVERNMENT COORDINATING COUNCIL.—The term “Energy Sector Government Coordinating Council” means the council consisting of representatives from relevant Federal Government agencies to provide effective coordination of energy sector efforts to ensure a secure, reliable, and resilient energy infrastructure and to carry out the role of the Government Coordinating Council as established in the National Infrastructure Protection Plan for the energy sector.

20 (5) HUMAN FACTORS RESEARCH.—The term
21 “human factors research” means research on human
22 performance in social and physical environments,
23 and on the integration of humans with physical systems and computer hardware and software.

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

7 (7) SECRETARY.—The term “Secretary” means
8 the Secretary of Energy.

9 (8) TRANSIENT DEVICES.—The term “transient
10 devices” means removable media, including floppy
11 disks, compact disks, USB flash drives, external
12 hard drives, mobile devices, and other devices that
13 utilize wireless connections for limited periods of
14 time.

15 **SEC. 4. ELECTRICITY SECTOR CYBERSECURITY RESEARCH,**
16 **DEVELOPMENT, AND DEMONSTRATION PRO-**
17 **GRAM.**

18 (a) IN GENERAL.—The Secretary, in coordination
19 with appropriate Federal agencies, the Electricity Sub-
20 sector Coordinating Council, State, tribal, local, and terri-
21 torial governments, private sector vendors, and other rel-
22 evant stakeholders, shall carry out a research, develop-
23 ment, and demonstration initiative to harden and mitigate
24 the electric grid from the consequences of cyber attacks
25 by increasing the cybersecurity capabilities of the elec-

1 tricity sector and accelerating the development of cyberse-
2 curity technologies and tools.

3 (b) DEPARTMENT OF ENERGY.—As part of the ini-
4 tiative described in subsection (a), the Secretary shall
5 carry out activities to—

6 (1) identify cybersecurity risks to the commu-
7 nication and control systems within, and impacting,
8 the electricity sector;

9 (2) develop methods and tools to rapidly detect
10 cyber intruders and cyber incidents, including the
11 use of data analytics techniques to validate and
12 verify system behavior using multiple data streams
13 reflecting the state of the system;

14 (3) assess emerging energy technology cyberse-
15 curity capabilities, and integrate cybersecurity fea-
16 tures and protocols into the design, development,
17 and deployment of emerging technologies, including
18 renewable energy technologies;

19 (4) develop secure industrial control system
20 protocols and identify vulnerabilities in existing pro-
21 tocols;

22 (5) work with manufacturers to build or retrofit
23 security features and protocols into—

24 (A) communication and network systems
25 and management processes;

1 (B) industrial control and energy manage-
2 ment system devices, components, software,
3 firmware, and hardware, including distributed
4 control and management systems and building
5 management systems;

6 (C) data storage systems and data man-
7 agement and analysis processes;

8 (D) generation, transmission, distribution,
9 and energy storage technologies;

10 (E) automated and manually controlled de-
11 vices and equipment for monitoring or man-
12 aging frequency, voltage, and current;

13 (F) technologies used to synchronize time
14 and develop guidance for operational contin-
15 ugency plans when time synchronization tech-
16 nologies are compromised;

17 (G) end user elements that connect to the
18 grid, including—

19 (i) meters, synchrophasors, and other
20 sensors;

21 (ii) distribution automation tech-
22 nologies, smart inverters, and other grid
23 control technologies;

24 (iii) distributed generation and energy
25 storage technologies;

- 1 (iv) demand response technologies;
- 2 (v) home and building energy control
- 3 systems;
- 4 (vi) electric and plug-in hybrid vehi-
- 5 cles; and
- 6 (vii) other relevant devices, software,
- 7 firmware, hardware, and distributed energy
- 8 technologies; and
- 9 (H) the supply chain of electric grid man-
- 10 agement system components;
- 11 (6) improve the physical security of communica-
- 12 tion technologies and industrial control systems, in-
- 13 cluding remote assets;
- 14 (7) integrate human factors research into the
- 15 design and development of advanced tools and proc-
- 16 esses for dynamic monitoring, detection, protection,
- 17 mitigation, and response;
- 18 (8) advance the capabilities and use of relevant
- 19 interdisciplinary mathematical and computer simula-
- 20 tion modeling and analysis methods;
- 21 (9) evaluate and understand the potential con-
- 22 sequences of practices used to maintain the cyberse-
- 23 curity of information technology systems on the cy-
- 24 bersecurity of industrial control systems;

1 (10) increase access to and the capabilities of
2 existing cybersecurity test beds to simulate impacts
3 of cyber attacks on industrial control system devices,
4 components, software, and hardware; and

5 (11) reduce the cost of implementing effective
6 cybersecurity technologies and tools in the electricity
7 sector.

8 (c) NATIONAL SCIENCE FOUNDATION.—The Na-
9 tional Science Foundation shall—

10 (1) support fundamental research to advance
11 cybersecurity applications, technologies, and tools for
12 industrial control systems, including incorporating
13 interdisciplinary research in—

14 (A) evolutionary systems, theories, mathe-
15 matics, and models;

16 (B) economic and financial theories, math-
17 ematics, and models; and

18 (C) big data analytical methods, mathe-
19 matics, computer coding, and algorithms; and

20 (2) support education and training for the in-
21 dustrial control system cybersecurity workforce, in-
22 cluding through the Advanced Technological Edu-
23 cation program, graduate research fellowships, and
24 other appropriate programs.

1 (d) DEPARTMENT OF HOMELAND SECURITY
2 SCIENCE AND TECHNOLOGY DIRECTORATE.—The Science
3 and Technology Directorate of the Department of Home-
4 land Security, in collaboration with the Department of En-
5 ergy, experts in the private sector with the necessary clear-
6 ances, and other relevant stakeholders, shall assess exist-
7 ing cybersecurity technologies and tools used in the de-
8 fense industry and—

9 (1) identify technologies and tools that could be
10 applied to meeting evolving civilian energy sector cy-
11 bersecurity needs;

12 (2) develop a research strategy that incor-
13 porates human factors research findings to guide the
14 modification of defense industry cybersecurity tools
15 for use in the civilian sector;

16 (3) develop a strategy to accelerate efforts to
17 bring modified defense industry cybersecurity tools
18 to the civilian market; and

19 (4) carry out other activities the Secretary of
20 Homeland Security considers appropriate to meet
21 the goals of this subsection.

1 **SEC. 5. TECHNICAL STANDARDS AND GUIDANCE DOCU-**
2 **MENTS FOR ELECTRICITY SECTOR CYBERSE-**
3 **CURITY RESEARCH.**

4 (a) IN GENERAL.—The Secretary, in coordination
5 with appropriate Federal agencies, the Electricity Sub-
6 sector Coordinating Council, standards development orga-
7 nizations, State, tribal, local, and territorial governments,
8 private sector vendors, and other relevant stakeholders,
9 shall coordinate the development of guidance documents
10 for research and demonstration activities to improve the
11 cybersecurity capabilities of the electricity sector through
12 participating agencies. As part of these activities, the Sec-
13 retary shall—

14 (1) facilitate stakeholder involvement to up-
15 date—

16 (A) the Roadmap to Achieve Energy Deliv-
17 ery Systems Cybersecurity (published in Sep-
18 tember 2011);

19 (B) the Cybersecurity Procurement Lan-
20 guage for Energy Delivery Systems (published
21 by the Energy Sector Control Systems Working
22 Group in April 2014), including developing
23 guidance for—

24 (i) contracting with third parties to
25 conduct vulnerability testing for industrial
26 control systems;

1 (ii) contracting with third parties that
2 will utilize transient devices to access in-
3 dustrial control or information technology
4 systems; and

5 (iii) managing supply chain risks; and

6 (C) the Electricity Subsector Cybersecurity
7 Capability Maturity Model (published by the
8 Department of Energy in February 2014), in-
9 cluding the development of—

10 (i) metrics to measure changes in cy-
11 bersecurity capabilities and assess the po-
12 tential for metrics to drive unexpected be-
13 havioral changes that would reduce secu-
14 rity; and

15 (ii) an analysis of incentive mecha-
16 nisms and their potential to increase in-
17 vestments in cybersecurity;

18 (2) develop voluntary guidance to improve fo-
19 rensic analyses capabilities, including—

20 (A) developing standardized terminology
21 and monitoring processes;

22 (B) identifying minimum data needed; and

23 (C) utilizing human factors research to de-
24 velop more effective procedures for logging inci-
25 dent events; and

1 (3) work with the National Science Foundation,
2 Department of Homeland Security, National Insti-
3 tute of Standards and Technology, and stakeholders
4 to develop a mechanism to anonymize, aggregate,
5 and share the testing results from cybersecurity in-
6 dustrial control system test beds to facilitate tech-
7 nology improvements by public and private sector re-
8 searchers.

9 (b) CRITICAL ELECTRIC INFRASTRUCTURE INFOR-
10 MATION.—Information provided to Federal agencies for
11 the purposes of carrying out subsection (a) shall be consid-
12 ered critical electric infrastructure information and pro-
13 vided the protections established in section 10.

14 (c) STANDARDS.—The Secretary, in collaboration
15 with the Director of the National Institute of Standards
16 and Technology and other appropriate Federal agencies,
17 shall convene relevant stakeholders and facilitate the de-
18 velopment of—

19 (1) voluntary, consensus-based technical stand-
20 ards to improve cybersecurity for—

21 (A) emerging energy technologies;

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

25 (C) electric vehicles; and

1 (D) other technologies and devices that
2 connect to the electric grid that can affect volt-
3 age stability;

4 (2) recommended cybersecurity features and re-
5 quirements that can be used by the private sector to
6 design and build interoperable cybersecurity features
7 into—

8 (A) devices and components;

9 (B) software and hardware; and

10 (C) other technologies that connect to the
11 electric grid; and

12 (3) voluntary standards for test beds and test
13 bed methodologies that will enable reproducible test-
14 ing of industrial control system devices, components,
15 software, and hardware across test beds.

16 **SEC. 6. VULNERABILITY TESTING AND TECHNICAL ASSIST-**
17 **ANCE TO INCREASE CYBERRESILIENCE.**

18 (a) IN GENERAL.—The Secretary shall—

19 (1) collaborate with electricity sector asset own-
20 ers and operators in the private sector, leveraging
21 the research facilities and expertise of the National
22 Laboratories, to—

23 (A) utilize a range of methods, including
24 voluntary vulnerability testing and red team-

1 blue team exercises, to identify vulnerabilities in
2 physical and cyber systems;

3 (B) develop cybersecurity risk assessment
4 tools and provide confidential analyses and rec-
5 ommendations to participating stakeholders;

6 (C) work with stakeholders to develop
7 methods to share anonymized and aggregated
8 results in a format that enables the electricity
9 sector, researchers, and the private sector to
10 advance cybersecurity efforts, technologies, and
11 tools; and

12 (D) leverage the unique strengths and ex-
13 pertise of the National Laboratories and Fed-
14 eral agencies;

15 (2) collaborate with relevant stakeholders to—

16 (A) identify information, research, staff
17 training, and analysis tools needed to evaluate
18 industrial control system cybersecurity issues
19 and challenges in the electricity sector; and

20 (B) facilitate the sharing of information
21 and the development of tools identified under
22 subparagraph (A);

23 (3) collaborate with and support electricity sec-
24 tor trade organizations and their research agencies

1 to improve the cybersecurity of industrial control
2 systems used by members and stakeholders; and

3 (4) collaborate with tribal governments to—

4 (A) identify information, research, and
5 analysis tools needed by tribal governments to
6 increase the industrial control system cyberse-
7 curity of electricity assets within their jurisdic-
8 tion; and

9 (B) facilitate the sharing of information
10 and the development of tools needed to ensure
11 the cybersecurity of tribal electricity assets and
12 systems.

13 (b) CRITICAL ELECTRIC INFRASTRUCTURE INFOR-
14 MATION.—Information provided to Federal agencies for
15 the purposes of carrying out subsection (a)(1)(C) shall be
16 considered critical electric infrastructure information and
17 provided the protections established in section 10.

18 **SEC. 7. EDUCATION AND WORKFORCE TRAINING RE-**
19 **SEARCH AND STANDARDS.**

20 (a) DEPARTMENT OF ENERGY.—The Secretary
21 shall—

22 (1) utilize human factors research and other
23 methods to identify core skills used by electricity
24 sector industrial control systems cybersecurity pro-
25 fessionals; and

1 (2) develop assessment methods and tools to
2 identify existing personnel that show competence in
3 the core skills identified under paragraph (1).

4 (b) NATIONAL INSTITUTE OF STANDARDS AND
5 TECHNOLOGY.—The Director of the National Institute of
6 Standards and Technology shall—

7 (1) develop voluntary, innovative industrial con-
8 trol systems cybersecurity training and retraining
9 standards, lessons, and recommendations for the
10 electricity sector that minimize duplication of cyber-
11 security compliance training programs; and

12 (2) maintain a public database of industrial
13 control systems cybersecurity education, training,
14 and certification programs.

15 **SEC. 8. INTERAGENCY COORDINATION AND STRATEGIC**
16 **PLAN FOR ELECTRICITY SECTOR CYBERSE-**
17 **CURITY RESEARCH.**

18 (a) DUTIES.—The Energy Sector Government Co-
19 ordinating Council shall—

20 (1) review the most recent version of the Road-
21 map to Achieve Energy Delivery Systems Cybersecu-
22 rity and identify crosscutting energy grid cybersecu-
23 rity research needs and opportunities for collabora-
24 tion among Federal agencies and between Federal
25 agencies and other relevant stakeholders;

1 (2) identify interdisciplinary research, tech-
2 nology, and tools that can be applied to industrial
3 control system cybersecurity challenges in the elec-
4 tricity sector;

5 (3) identify technology transfer opportunities to
6 accelerate the development and commercial applica-
7 tion of novel industrial control system cybersecurity
8 technologies, systems, and processes; and

9 (4) develop a coordinated Interagency Strategic
10 Plan to advance cybersecurity capabilities for indus-
11 trial control systems used in the electricity sector
12 that builds on the Roadmap to Achieve Energy De-
13 livery Systems in Cybersecurity.

14 (b) STRATEGIC PLAN.—

15 (1) SUBMITTAL.—The Interagency Strategic
16 Plan developed under subsection (a)(4) shall be sub-
17 mitted to Congress within 12 months after the date
18 of enactment of this Act.

19 (2) CONTENTS.—The Interagency Strategic
20 Plan shall include—

21 (A) an analysis of how existing cybersecu-
22 rity research efforts conducted by member
23 agencies are coordinated and can complement
24 and advance the goals of the Roadmap to

1 Achieve Energy Delivery Systems Cybersecu-
2 rity;

3 (B) recommendations for prioritized re-
4 search efforts that could contribute to advanc-
5 ing the cybersecurity of electricity sector indus-
6 trial control systems;

7 (C) a description of how existing and pro-
8 posed public and private sector research efforts
9 address the topics described in paragraph (3);
10 and

11 (D) a description of needed support for
12 workforce training in this area.

13 (3) CONSIDERATION.—In developing the Inter-
14 agency Strategic Plan, the Energy Sector Govern-
15 ment Coordinating Council shall consider—

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

20 (B) contributions of other disciplines to the
21 development of innovative cybersecurity proto-
22 cols, devices, components, technologies, and
23 tools;

24 (C) opportunities for Small Business Inno-
25 vation Research (SBIR) and other technology

1 transfer programs to facilitate private sector
2 development of industrial control system cyber-
3 security protocols, devices, components, tech-
4 nologies, and tools;

5 (D) broader applications of the work done
6 by relevant Federal agencies to advance the cy-
7 bersecurity of industrial control systems used
8 by other sectors; and

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

14 (c) MEMBERSHIP.—For the purposes of carrying out
15 this section, the Energy Sector Government Coordinating
16 Council shall include representatives from Federal agen-
17 cies with expertise in industrial control systems cybersecu-
18 rity, information technology cybersecurity, cyber physical
19 systems, engineering, human factors research, human-ma-
20 chine interfaces, high performance computing, big data
21 and data analytics, or other disciplines considered appro-
22 priate by the Council Chair. The Chair shall consider in-
23 cluding at least one employee designated by the head of
24 each of the following agencies:

25 (1) In the Department of Energy—

1 (A) the Office of Electricity Delivery and
2 Energy Reliability;

3 (B) the Office of Science's Advanced Sci-
4 entific Computing Research program;

5 (C) the Office of Small Business Innova-
6 tion Research/Small Business Technology
7 Transfer programs;

8 (D) the Office of Technology Transitions;
9 and

10 (E) other offices considered appropriate by
11 the Secretary.

12 (2) The National Science Foundation.

13 (3) The Department of Homeland Security's
14 Science and Technology Directorate.

15 (4) The National Institute of Standards and
16 Technology.

17 (5) The National Aeronautics and Space Ad-
18 ministration's Human Research Program.

19 (6) The Office of Science and Technology Pol-
20 icy.

21 (7) The Federal Energy Regulatory Commis-
22 sion.

23 **SEC. 9. REPORTS TO CONGRESS.**

24 (a) IDENTIFICATION OF COMMON FACTORS IN
25 CYBER ATTACKS.—

1 (1) STUDY.—The Secretary, in collaboration
2 with the Secretary of Homeland Security, other ap-
3 propriate Federal agencies, and energy sector stake-
4 holders, shall conduct a study to analyze cyber at-
5 tacks on electricity sector industrial control systems
6 and identify cost-effective opportunities to improve
7 cybersecurity.

8 (2) CRITICAL ELECTRIC INFRASTRUCTURE IN-
9 FORMATION.—Incident data provided to Federal
10 agencies for the purposes of carrying out this sub-
11 section shall be considered critical electric infrastruc-
12 ture information and provided the protections estab-
13 lished in section 10.

14 (3) CONTENT.—The study shall—

15 (A) summarize cyber incident data pro-
16 vided to the Secretary by relevant Federal agen-
17 cies and energy sector stakeholders;

18 (B) analyze processes, operational proce-
19 dures, and other factors common among cyber
20 attacks;

21 (C) identify the points where human be-
22 havior played a critical role in maintaining or
23 compromising the security of the system;

24 (D) recommend—

1 (i) changes to the design of devices,
2 human-machine interfaces, technologies,
3 and tools to optimize security that do not
4 require a change in human behavior;

5 (ii) changes to processes or oper-
6 ational procedures that do not require a
7 change in human behavior; and

8 (iii) training techniques to increase
9 the capacity of employees to actively iden-
10 tify, prevent, or neutralize the impact of
11 cyber attacks; and

12 (E) evaluate existing engineering and tech-
13 nical design criteria and guidelines that incor-
14 porate human factors research findings, and
15 recommend criteria and guidelines for industrial
16 control system cybersecurity tools that can be
17 used to develop procurement guidance, includ-
18 ing guidance for alarms, displays, and layouts.

19 (4) CONSULTATION.—In conducting the study,
20 the Secretary shall consult with electricity sector
21 stakeholders, professionals with expertise in human
22 factors research, private sector industrial control
23 system vendors, and other relevant parties.

24 (5) REPORT.—Not later than 24 months after
25 the date of enactment of this Act, the Secretary

1 shall submit to the Committee on Science, Space,
2 and Technology of the House of Representatives and
3 the Committee on Energy and Natural Resources of
4 the Senate a report on the results of the study, in-
5 cluding the findings of the Secretary on each of the
6 items described in paragraph (3).

7 (b) BALANCING RISKS, SECURITY, AND MODERNIZA-
8 TION OF INDUSTRIAL SYSTEMS.—

9 (1) STUDY.—The Secretary, in collaboration
10 with the National Institute of Standards and Tech-
11 nology, other Federal agencies, and electricity sector
12 stakeholders, shall examine the risks associated with
13 increasing penetration of digital technologies in
14 operational networks.

15 (2) CONTENT.—The study shall—

16 (A) evaluate the relative qualitative risks
17 and benefits of various design and architecture
18 options for electricity sector industrial control
19 systems, including consideration of—

20 (i) designs that include both digital
21 and analog control devices and tech-
22 nologies;

23 (ii) different communication tech-
24 nologies used to move information and

1 data between control system devices, tech-
2 nologies, and system operators;

3 (iii) automated and human-in-the-loop
4 devices and technologies;

5 (iv) programmable versus non-
6 programmable devices and technologies;
7 and

8 (v) increased redundancy using dis-
9 similar cybersecurity technologies;

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

13 (C) provide recommendations for research,
14 development, demonstration, and commercial
15 application activities to address issues raised in
16 subparagraphs (A) and (B); and

17 (D) recommend guidance to minimize over-
18 all system risks.

19 (3) CONSULTATION.—In conducting the study,
20 the Secretary shall consult with electricity sector
21 stakeholders, academic and private sector research-
22 ers, private sector industrial control system vendors,
23 and other relevant parties.

24 (4) REPORT.—Not later than 24 months after
25 the date of enactment of this Act, the Secretary

1 shall submit to the Committee on Science, Space,
2 and Technology of the House of Representatives and
3 the Committee on Energy and Natural Resources of
4 the Senate a report on the results of the study, in-
5 cluding the findings of the Secretary on each of the
6 items described in paragraph (2).

7 **SEC. 10. PROTECTION OF CRITICAL ELECTRIC INFRA-**
8 **STRUCTURE INFORMATION.**

9 Any Federal agency that produces information or has
10 information made available to it in the course of carrying
11 out this Act shall determine whether to designate any such
12 information as critical electric infrastructure information.
13 Critical electric infrastructure information—

14 (1) shall be exempt from disclosure under sec-
15 tion 552(b)(3) of title 5, United States Code; and

16 (2) shall not be made available by any Federal,
17 State, political subdivision, or tribal authority pursu-
18 ant to any Federal, State, political subdivision, or
19 tribal law requiring public disclosure of information
20 or records.

21 **SEC. 11. AUTHORIZATION OF APPROPRIATIONS.**

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

24 (1) \$65,100,000 for fiscal year 2017;

25 (2) \$68,355,000 for fiscal year 2018;

- 1 (3) \$71,773,000 for fiscal year 2019;
- 2 (4) \$75,361,000 for fiscal year 2020; and
- 3 (5) \$79,129,000 for fiscal year 2021.

○