

Union Calendar No. 501

112TH CONGRESS
2^D SESSION

H. R. 3674

[Report No. 112-592, Part I]

To amend the Homeland Security Act of 2002 to make certain improvements in the laws relating to cybersecurity, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

DECEMBER 15, 2011

Mr. DANIEL E. LUNGREN of California (for himself, Mr. KING of New York, Mr. MCCAUL, Mr. BILIRAKIS, Mrs. MILLER of Michigan, Mr. WALBERG, Mr. MARINO, Mr. LONG, Mr. TURNER of New York, Mr. STIVERS, and Mr. LANGEVIN) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committees on Oversight and Government Reform, Science, Space, and Technology, the Judiciary, and Select Intelligence (Permanent Select), 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

JULY 11, 2012

Reported from the Committee on Homeland Security with an amendment

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

JULY 11, 2012

The Committees on Oversight and Government Reform, Science, Space, and Technology, the Judiciary, and the Permanent Select Committee on Intelligence discharged; referred to the Committee on Energy and Commerce for a period ending not later than September 21, 2012, for consideration of such provisions of the bill and amendment as fall within the jurisdiction of that committee pursuant to clause 1(f) of rule X.

SEPTEMBER 21, 2012

Additional sponsor: Mr. MEEHAN

SEPTEMBER 21, 2012

Deleted sponsor: Mr. LANGEVIN (added December 15, 2011; deleted April 25, 2012)

SEPTEMBER 21, 2012

The Committee on Energy and Commerce 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 December 15, 2011]

A BILL

To amend the Homeland Security Act of 2002 to make certain improvements in the laws relating to cybersecurity, 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 “Promoting and Enhanc-*
5 *ing Cybersecurity and Information Sharing Effectiveness*
6 *Act of 2012” or the “PRECISE Act of 2012”.*

7 **SEC. 2. DEPARTMENT OF HOMELAND SECURITY CYBERSE-**
8 **CURITY ACTIVITIES.**

9 *(a) IN GENERAL.—Subtitle C of title II of the Home-*
10 *land Security Act of 2002 is amended by adding at the end*
11 *the following new sections:*

12 **“SEC. 226. DEPARTMENT OF HOMELAND SECURITY CYBER-**
13 **SECURITY ACTIVITIES.**

14 *“(a) IN GENERAL.—The Secretary shall perform nec-*
15 *essary activities to help facilitate the protection of Federal*
16 *systems and, solely upon the request of critical infrastruc-*
17 *ture owners and operators, assist such critical infrastruc-*
18 *ture owners and operators in protecting their critical infra-*
19 *structure information systems to include—*

20 *“(1) conduct risk assessments, subject to the*
21 *availability of resources and, solely upon request from*
22 *critical infrastructure owners and operators, critical*
23 *infrastructure information systems;*

24 *“(2) assist in fostering the development, in con-*
25 *junction with the National Institute of Standards and*

1 *Technology and other Federal departments and agen-*
2 *cies and the private sector, of essential information*
3 *security technologies and capabilities for protecting*
4 *Federal systems and critical infrastructure informa-*
5 *tion systems, including comprehensive protective ca-*
6 *pabilities and other technological solutions;*

7 *“(3) assist in efforts to mitigate communications*
8 *and information technology supply chain*
9 *vulnerabilities;*

10 *“(4) support nationwide awareness and outreach*
11 *efforts, to include participation in appropriate inter-*
12 *agency cybersecurity awareness and education pro-*
13 *grams, to educate the public;*

14 *“(5) conduct exercises, simulations, and other ac-*
15 *tivities designed to support and evaluate the national*
16 *cyber incident response plan; and*

17 *“(6) subject to the availability of resources and,*
18 *upon request of critical infrastructure owners and op-*
19 *erators, provide technical assistance, including send-*
20 *ing on-site teams, to such critical infrastructure own-*
21 *ers and operators.*

22 *“(b) INTERAGENCY DUTIES.—At the direction of the*
23 *Office of Management and Budget pursuant to subchapter*
24 *II of chapter 35 of title 44, United States Code, the Sec-*
25 *retary shall—*

1 “(1) conduct targeted risk assessments and oper-
2 ational evaluations, in conjunction with the heads of
3 other agencies, for Federal systems that may include
4 threat, vulnerability, and impact assessments and
5 penetration testing;

6 “(2) in conjunction with the National Institute
7 of Standards and Technology and appropriate Fed-
8 eral departments and agencies, as well as the private
9 sector, provide for the use of consolidated intrusion
10 detection, prevention, or other protective capabilities
11 and use associated countermeasures for the purpose of
12 protecting Federal systems from cybersecurity threats;

13 “(3) in conjunction with other agencies and the
14 private sector, assess and foster the development of in-
15 formation security technologies and capabilities for
16 use and dissemination throughout the Department of
17 Homeland Security and to be made available across
18 multiple agencies;

19 “(4) designate an entity within the Department
20 of Homeland Security to receive reports and informa-
21 tion about cybersecurity incidents, threats, and
22 vulnerabilities affecting Federal systems; and

23 “(5) provide incident detection, analysis, mitiga-
24 tion, and response information and remote or on-site
25 technical assistance for Federal systems.

1 “(c) *CYBERSECURITY OPERATIONAL ACTIVITY.*—

2 “(1) *IN GENERAL.*—While carrying out the re-
3 responsibilities authorized in paragraphs (2) and (3) of
4 subsection (b), the Secretary is authorized, notwith-
5 standing any other provision of law, to acquire, inter-
6 cept, retain, use, and disclose communications and
7 other system traffic that are transiting to or from or
8 stored on Federal systems and to deploy counter-
9 measures with regard to such communications and
10 system traffic for cybersecurity purposes if the Sec-
11 retary certifies that—

12 “(A) such acquisitions, interceptions, and
13 countermeasures are reasonably necessary for the
14 purpose of protecting Federal systems from cy-
15 bersecurity threats;

16 “(B) the content of communications will be
17 collected and retained only when the communica-
18 tion is associated with a known or reasonably
19 suspected cybersecurity threat and communica-
20 tions and system traffic will not be subject to the
21 operation of a countermeasure unless associated
22 with such threats;

23 “(C) information obtained pursuant to ac-
24 tivities authorized under this subsection will
25 only be retained, used, or disclosed to protect

1 *Federal systems from cybersecurity threats, miti-*
2 *gate against such threats, or, with the approval*
3 *of the Attorney General, for law enforcement*
4 *purposes when the information is evidence of a*
5 *crime which has been, is being, or is about to be*
6 *committed;*

7 “(D) notice has been provided to users of
8 *Federal systems concerning the potential for ac-*
9 *quisition, interception, retention, use, and disclo-*
10 *sure of communications and other system traffic;*
11 *and*

12 “(E) such activities are implemented pursu-
13 *ant to policies and procedures governing the ac-*
14 *quisition, interception, retention, use, and disclo-*
15 *sure of communications and other system traffic*
16 *that have been reviewed and approved by the At-*
17 *torney General.*

18 “(2) *OBTAINING ASSISTANCE.—The Secretary*
19 *may enter into contracts or other agreements, or oth-*
20 *erwise request and obtain the assistance of, private*
21 *entities that provide electronic communication or cy-*
22 *bersecurity services to acquire, intercept, retain, use,*
23 *and disclose communications and other system traffic*
24 *consistent with paragraph (1).*

1 “(3) *PERMISSION BY OTHER AGENCIES.*—Agen-
2 cies are authorized to permit the Secretary, or a pri-
3 vate entity providing assistance to the Secretary
4 under paragraph (2), to acquire, intercept, retain,
5 use, or disclose communications, system traffic,
6 records, or other information transiting to or from or
7 stored on a Federal system, notwithstanding any
8 other provision of law, for the purpose of protecting
9 Federal systems from cybersecurity threats or miti-
10 gating such threats in connection with activities
11 under this subsection.

12 “(4) *PRIVILEGED COMMUNICATIONS.*—No other-
13 wise privileged communication obtained in accord-
14 ance with, or in violation of, this subtitle shall lose
15 its privileged character.

16 “(d) *COORDINATION.*—

17 “(1) *COORDINATION WITH OTHER ENTITIES.*—In
18 carrying out cybersecurity activities subsection (a),
19 the Secretary shall coordinate, as appropriate, with—

20 “(A) the head of relevant Federal depart-
21 ments or agencies;

22 “(B) representatives of State and local gov-
23 ernments;

24 “(C) owners and operators of critical infra-
25 structure;

1 “(D) suppliers of technology for owners and
2 operators of critical infrastructure;

3 “(E) academia; and

4 “(F) international organizations and for-
5 eign partners.

6 “(2) LEAD DHS CYBERSECURITY OFFICIAL.—The
7 Secretary shall designate a lead cybersecurity official
8 within the Department to provide leadership to the
9 cybersecurity activities of the Department and to en-
10 sure that the Department’s cybersecurity activities
11 under this subtitle are coordinated with all other in-
12 frastructure protection and cyber-related programs
13 and activities of the Department, including those of
14 any intelligence or law enforcement components or
15 entities within the Department.

16 “(3) REPORTS TO CONGRESS.—The lead DHS
17 cybersecurity official shall make annual reports to the
18 appropriate committees of Congress on the coordina-
19 tion of cyber-related programs across the Department.

20 “(e) STRATEGY.—In carrying out the cybersecurity ac-
21 tivities of the Department under subsection (a), the Sec-
22 retary shall develop and maintain a strategy that—

23 “(1) articulates the actions of the Department
24 that are necessary to assure the readiness, reliability,

1 *continuity, integrity, and resilience of Federal sys-*
2 *tems and critical infrastructure information systems;*

3 *“(2) includes explicit goals and objectives for the*
4 *Department as well as specific timeframes for*
5 *achievement of stated goals and objectives by the De-*
6 *partment;*

7 *“(3) fosters the continued superiority and reli-*
8 *ability of the United States information technology*
9 *and communications sectors; and*

10 *“(4) ensures that activities of the Department*
11 *are undertaken in a manner that protects statutory*
12 *privacy rights and civil liberties of United States per-*
13 *sons.*

14 *“(f) NO RIGHT OR BENEFIT.—The provision of assist-*
15 *ance or information to critical infrastructure owners and*
16 *operators, upon request of such critical infrastructure own-*
17 *ers and operators, under this section shall be at the discre-*
18 *tion of the Secretary and subject to the availability of re-*
19 *sources. The provision of certain assistance or information*
20 *to one critical infrastructure owner or and operator pursu-*
21 *ant to this section shall not create a right or benefit, sub-*
22 *stantive or procedural, to similar assistance or information*
23 *for any other critical infrastructure owner or and operator.*

24 *“(g) PRIVACY OFFICER OVERSIGHT.—The Privacy Of-*
25 *ficer of the Department of Homeland Security shall review*

1 *on an ongoing basis, and prepare, as necessary, privacy*
2 *impact assessments on, the cybersecurity policies, programs,*
3 *and activities of the Department of Homeland Security for*
4 *such purposes as ensuring compliance with all relevant con-*
5 *stitutional and legal protections.*

6 “(h) SAVINGS CLAUSE.—Nothing in this subtitle shall
7 be interpreted to—

8 “(1) alter or amend the authorities of any Fed-
9 eral department or agency other than the Department
10 of Homeland Security, including the law enforcement
11 or intelligence authorities of any such Federal depart-
12 ment or agency or the authority of any such Federal
13 department or agency to protect sources and methods
14 and the national security;

15 “(2) limit or modify an existing information
16 sharing or other relationship;

17 “(3) prohibit a new information sharing or other
18 relationship;

19 “(4) require a new information sharing or other
20 relationship between the Federal Government and a
21 private sector entity;

22 “(5) alter or otherwise limit the authority of any
23 Federal department or agency to also undertake any
24 activities that the Department of Homeland Security
25 is authorized to undertake pursuant to this section; or

1 “(6) provide additional authority to, or modify
2 an existing authority of the Department of Homeland
3 Security to control, modify, require, or otherwise di-
4 rect the cybersecurity efforts of a private-sector entity
5 or a component of the Federal Government or a State,
6 local, or tribal government.

7 “(i) *DEFINITIONS.*—In this section:

8 “(1) The term ‘countermeasure’ means auto-
9 mated actions with defensive intent to modify or block
10 data packets associated with electronic or wire com-
11 munications, internet traffic, program code, or other
12 system traffic transiting to or from or stored on an
13 information system for the purpose of protecting the
14 information system from cybersecurity threats.

15 “(2) The term ‘Federal systems’ means informa-
16 tion systems owned, operated, leased, or otherwise
17 controlled by a Federal department or agency, or on
18 behalf of a Federal department or agency, except for
19 national security systems or those information sys-
20 tems under the control of, used by, or storing infor-
21 mation of the Department of Defense or any element
22 of the Intelligence Community, including any infor-
23 mation systems used or operated by a contractor of
24 the Department of Defense or any element of the In-
25 telligence Community, or other organization on behalf

1 *of the Department of Defense or any element of the*
2 *Intelligence Community.*

3 “(3) *The term ‘critical infrastructure informa-*
4 *tion systems’ means any information system that is—*

5 “(A) *vital to the functioning of critical in-*
6 *frastructure as defined in section 5195c(e) of title*
7 *42, United States Code; or*

8 “(B) *owned or operated by or on behalf of*
9 *a State or local government entity that is nec-*
10 *essary to ensure essential government operations*
11 *continue.*

12 “(4) *The term ‘information system’ means any*
13 *equipment or interconnected system or subsystem of*
14 *equipment that is used in the automatic acquisition,*
15 *storage, manipulation, management, movement, con-*
16 *trol, display, switching, interchange, transmission, or*
17 *reception of data or information, and includes—*

18 “(A) *computers and computer networks;*

19 “(B) *ancillary equipment;*

20 “(C) *software, firmware, and related proce-*
21 *dures;*

22 “(D) *services, including support services;*

23 *and*

24 “(E) *related resources.*

1 “(5) *The term ‘national security system’ means*
2 *any information infrastructure (including any tele-*
3 *communications system) used or operated by an agen-*
4 *cy, by a contractor of an agency, or by another orga-*
5 *nization on behalf of an agency—*

6 “(A) *the function, operation, or use of*
7 *which—*

8 “(i) *involves intelligence activities or*
9 *intelligence-related activities;*

10 “(ii) *involves cryptologic activities re-*
11 *lated to national security;*

12 “(iii) *involves command and control of*
13 *military forces;*

14 “(iv) *involves equipment that is an in-*
15 *tegral part of a weapon or weapons system;*
16 *or*

17 “(v) *is critical to the direct fulfillment*
18 *of military or intelligence missions;*

19 “(B) *that contains information related to*
20 *the activities and other matters set forth in sub-*
21 *paragraph (A); or*

22 “(C) *that is protected by procedures estab-*
23 *lished for classified, national security, foreign*
24 *policy, intelligence or intelligence-related, or*
25 *other appropriate information.*

1 **“SEC. 227. PERSONNEL AUTHORITIES RELATED TO THE OF-**
2 ****FICE OF CYBERSECURITY AND COMMUNICA-****
3 ****TIONS.****

4 “(a) *IN GENERAL.*—*In order to assure that the De-*
5 *partment has the necessary resources to carry out the mis-*
6 *sion set forth in section 226, the Secretary may, as nec-*
7 *essary, convert competitive service positions, and the in-*
8 *cumbents of such positions, within the Office of Cybersecu-*
9 *rity and Communications to excepted service, or may estab-*
10 *lish new positions within the Office of Cybersecurity and*
11 *Communications in the excepted service, to the extent that*
12 *the Secretary determines such positions are necessary to*
13 *carry out the cybersecurity functions of the Department.*

14 “(b) *COMPENSATION.*—*The Secretary may—*

15 “(1) *fix the compensation of individuals who*
16 *serve in positions referred to in subsection (a) in rela-*
17 *tion to the rates of pay provided for comparable posi-*
18 *tions in the Department and subject to the same limi-*
19 *tations on maximum rates of pay established for em-*
20 *ployees of the Department by law or regulations; and*

21 “(2) *provide additional forms of compensation,*
22 *including benefits, incentives, and allowances, that*
23 *are consistent with and not in excess of the level au-*
24 *thorized for comparable positions authorized under*
25 *title 5, United States Code.*

1 “(c) *RETENTION BONUSES.*—*Notwithstanding any*
2 *other provision of law, the Secretary may pay a retention*
3 *bonus to any employee appointed under this section, if the*
4 *Secretary determines that the bonus is needed to retain es-*
5 *sential personnel. Before announcing the payment of a*
6 *bonus under this subsection, the Secretary shall submit a*
7 *written explanation of such determination to the Committee*
8 *on Homeland Security of the House of Representatives and*
9 *the Committee on Homeland Security and Governmental*
10 *Affairs of the Senate.*

11 “(d) *ANNUAL REPORT.*—*Not later than one year after*
12 *the date of the enactment of this section, and annually*
13 *thereafter, the Secretary shall submit to appropriate Con-*
14 *gressional committees a detailed report that includes, for*
15 *the period covered by the report—*

16 “(1) *a discussion the Secretary’s use of the flexi-*
17 *ble authority authorized under this section to recruit*
18 *and retain qualified employees;*

19 “(2) *metrics on relevant personnel actions, in-*
20 *cluding—*

21 “(A) *the number of qualified employees*
22 *hired by occupation and grade, level, or pay*
23 *band;*

24 “(B) *the total number of veterans hired;*

1 “(C) *the number of separations of qualified*
2 *employees;*

3 “(D) *the number of retirements of qualified*
4 *employees; and*

5 “(E) *the number and amounts of recruit-*
6 *ment, relocation, and retention incentives paid*
7 *to qualified employees by occupation and grade,*
8 *level, or pay band; and*

9 “(3) *long-term and short-term strategic goals to*
10 *address critical skills deficiencies, including an anal-*
11 *ysis of the numbers of and reasons for attrition of em-*
12 *ployees and barriers to recruiting and hiring individ-*
13 *uals qualified in cybersecurity.*

14 **“SEC. 228. FEDERAL PREEMPTION, EXCLUSIVITY, AND LAW**
15 **ENFORCEMENT AND INTELLIGENCE ACTIVI-**
16 **TIES.**

17 “(a) *PREEMPTION.—This subtitle supersedes any stat-*
18 *ute of a State or political subdivision of a State that re-*
19 *stricts or otherwise expressly regulates the acquisition,*
20 *interception, retention, use, or disclosure of communica-*
21 *tions, records, or other information by private entities or*
22 *governmental entities to the extent such statute is incon-*
23 *sistent with this subtitle.*

24 “(b) *ADDITIONAL EXCLUSIVE MEANS.—Section 226(c)*
25 *constitutes an additional exclusive means for the domestic*

1 *interception of wire or electronic communications, in ac-*
 2 *cordance with the provisions of law codified at section*
 3 *1812(b) of title 50, United States Code.*

4 “(c) *LIMITATION.*—*This subtitle does not authorize the*
 5 *Secretary to engage in law enforcement or intelligence ac-*
 6 *tivities that the Department is not otherwise authorized to*
 7 *conduct under existing law.”.*

8 (b) *CLERICAL AMENDMENT.*—*The table of contents in*
 9 *section 1(b) of such Act is amended by inserting after the*
 10 *item relating to section 225 the following new items:*

“Sec. 226. *Department of Homeland Security cybersecurity activities.*

“Sec. 227. *Personnel authorities related to the Office of Cybersecurity and Com-*
munications.

“Sec. 228. *Federal preemption, exclusivity, and law enforcement and intelligence*
activities.”.

11 (c) *PLAN FOR EXECUTION OF AUTHORITIES.*—*Not*
 12 *later than 120 days after the date of the enactment of this*
 13 *Act, the Secretary of Homeland Security shall submit to*
 14 *the Committee on Homeland Security of the House of Rep-*
 15 *resentatives and the Committee on Homeland Security and*
 16 *Governmental Affairs of the Senate a report containing a*
 17 *plan for the execution of the authorities contained in the*
 18 *amendment made by subsection (a).*

19 **SEC. 3. DEPARTMENT OF HOMELAND SECURITY CYBERSE-**
 20 **CURITY INFORMATION SHARING.**

21 (a) *DEPARTMENT OF HOMELAND SECURITY CYBERSE-*
 22 *CURITY INFORMATION SHARING.*—

1 (1) *IN GENERAL.*—Title II of the Homeland Se-
2 curity Act of 2002, as amended by section 2, is fur-
3 ther amended by adding at the end the following:

4 **“Subtitle E—Department of Home-**
5 **land Security Cybersecurity In-**
6 **formation Sharing**

7 **“SEC. 241. INFORMATION SHARING.**

8 *“The Secretary shall make appropriate cyber threat*
9 *information obtained by the Department pursuant to title*
10 *XI of the National Security Act of 1947 or other informa-*
11 *tion appropriately in the possession of the Department*
12 *available to appropriate owners and operators of critical*
13 *infrastructure on a timely basis consistent with the statu-*
14 *tory and other appropriate restrictions on the dissemina-*
15 *tion of such information and with the responsibilities of the*
16 *Secretary under this title.*

17 **“SEC. 242. ESTABLISHMENT OF NATIONAL CYBERSECURITY**
18 **AND COMMUNICATIONS INTEGRATION CEN-**
19 **TER.**

20 *“(a) ESTABLISHMENT.*—There is established within
21 *the Department the National Cybersecurity and Commu-*
22 *nications Integration Center.*

23 *“(b) PURPOSE.*—The center established pursuant to
24 *subsection (a) shall be the primary entity within the De-*
25 *partment for sharing timely cyber threat information and*

1 *exchanging technical assistance, advice, and support with*
2 *appropriate entities pursuant to the Department’s authori-*
3 *ties.*

4 **“SEC. 243. BOARD OF ADVISORS.**

5 “(a) *IN GENERAL.*—*The National Cybersecurity and*
6 *Communications Integration Center shall have a board of*
7 *advisors which shall advise the Secretary on the efficient*
8 *operation of the National Cybersecurity and Communica-*
9 *tions Integration Center.*

10 “(b) *COMPOSITION.*—*The board shall be composed of*
11 *13 members, including the following:*

12 “(1) *Eleven representatives from the critical in-*
13 *frastructure sectors enumerated in the National Infra-*
14 *structure Protection Plan, of which at least one mem-*
15 *ber shall represent a small business interest and at*
16 *least one member shall represent each of the following*
17 *sectors:*

18 “(A) *Banking and finance.*

19 “(B) *Communications.*

20 “(C) *Defense industrial base.*

21 “(D) *Energy, electricity subsector.*

22 “(E) *Energy, oil, and natural gas subsector.*

23 “(F) *Health care and public health.*

24 “(G) *Information technology.*

25 “(H) *Water.*

1 “(I) *Chemical.*

2 “(2) *Two representatives from the privacy and*
3 *civil liberties community.*

4 “(3) *The Chair of the National Council of Infor-*
5 *mation Sharing and Analysis Centers.*

6 “(c) *INITIAL APPOINTMENT.—Not later than 30 days*
7 *after the date of the enactment of this subtitle, the Secretary*
8 *of Homeland Security, in consultation with the heads of*
9 *the sector specific agencies of the critical infrastructure sec-*
10 *tors enumerated in the National Infrastructure Protection*
11 *Plan, shall appoint the members of the board described*
12 *under subsection (b) from individuals identified by the sec-*
13 *tor coordinating councils of the critical infrastructure sec-*
14 *tors enumerated in the National Infrastructure Protection*
15 *Plan.*

16 “(d) *TERMS.—*

17 “(1) *CRITICAL INFRASTRUCTURE REPRESENTA-*
18 *TIVES.—Each member of the board described in sub-*
19 *section (b)(1) shall be appointed for a term that is*
20 *not less than one year and not longer than three years*
21 *from the date of the member’s appointment, as deter-*
22 *mined by the member’s sector coordinating council.*

23 “(2) *OTHER REPRESENTATIVES.—Each member*
24 *of the board described in subsection (b)(2) or (3) shall*
25 *serve an initial term that is not less than two years*

1 *and not longer than three years from the date of the*
2 *member’s appointment, and each such member shall*
3 *select the member’s successor.*

4 “(e) *DUTIES.—The board shall—*

5 “(1) *meet not less frequently than quarterly;*

6 “(2) *act as an advocate on behalf of the private*
7 *sector in improving the operations of the National*
8 *Cybersecurity Communications Integration Center;*
9 *and*

10 “(3) *submit to the Secretary and the appropriate*
11 *committees of Congress the annual report described in*
12 *section 247.*

13 “(f) *ACCESS TO INFORMATION.—The members of the*
14 *board shall, subject to the laws and procedures applicable*
15 *to national security background investigations and security*
16 *clearances, be provided with the appropriate security clear-*
17 *ances and have access to appropriate information shared*
18 *with the National Cybersecurity and Communications Inte-*
19 *gration Center and shall be subject to all of the limitations*
20 *on the use of such information.*

21 “(g) *SUB-BOARDS.—The board shall have the authority*
22 *to constitute such sub-boards, or other advisory groups or*
23 *panels, as may be necessary to assist the board in carrying*
24 *out its functions under this section.*

1 **“SEC. 244. CHARTER.**

2 *“The Secretary shall develop a charter to govern the*
3 *operations and administration of the National Cybersecu-*
4 *rity and Communications Integration Center consistent*
5 *with the requirements of title XI of the National Security*
6 *Act of 1947. The charter shall include each of the following:*

7 *“(1) The organizational structure of the National*
8 *Cybersecurity and Communications Integration Cen-*
9 *ter, including a delineation of the mission expecta-*
10 *tions and responsibilities of the various elements as-*
11 *signed to the Center.*

12 *“(2) A mission statement of the National Cyber-*
13 *security and Communications Integration Center.*

14 *“(3) A plan that promotes broad participation*
15 *by large, medium, and small business owners and op-*
16 *erators of networks or systems in the private sector,*
17 *entities operating critical infrastructure, educational*
18 *institutions, State, tribal, and local governments, and*
19 *the Federal Government.*

20 *“(4) Procedures for making appropriate cyber*
21 *incident information available to outside groups for*
22 *academic research and insurance actuarial purposes.*

23 **“SEC. 245. PARTICIPATION.**

24 *“Not later than 90 days after the date of the enactment*
25 *of this subtitle, the Secretary shall publish the criteria and*
26 *procedures for voluntary participation and voluntary phys-*

1 ical collocation by appropriate Federal, State and local gov-
2 ernment departments, agencies and entities, and private
3 sector businesses and organizations within the National Cy-
4 bersecurity and Communications Integration Center.

5 **“SEC. 246. ANNUAL REPORT.**

6 *“The board of advisors of the National Cybersecurity*
7 *Communications Integration Center shall submit to the*
8 *Secretary and the appropriate committees of Congress an*
9 *annual report on the status of the National Cybersecurity*
10 *Communications Integration Center and how the Center ac-*
11 *complished its purpose under section 242 during the year*
12 *covered by the report. Each such report shall include, for*
13 *the year covered by the report—*

14 *“(1) information on the amount and nature of*
15 *information shared by and through the Center;*

16 *“(2) the number of violations of statutory infor-*
17 *mation sharing restrictions and the procedures estab-*
18 *lished for the Center and any steps taken by the Cen-*
19 *ter to reduce and eliminate such violations;*

20 *“(3) any changes to the Center’s charter as*
21 *agreed upon by the board and the membership; and*

22 *“(4) proposed ways to improve information*
23 *sharing by and through the Center.*

1 **“SEC. 247. AUTHORITY TO ISSUE WARNINGS.**

2 *“The Secretary may, in coordination with appropriate*
3 *Federal departments and agencies, provide advisories,*
4 *alerts, and warnings to relevant companies, targeted sec-*
5 *tors, other government entities, or the general public regard-*
6 *ing potential cybersecurity threats as appropriate. In*
7 *issuing such an advisory, alert, or warning, the Secretary*
8 *shall not disclose—*

9 *“(1) without the express consent of an entity vol-*
10 *untarily sharing information with the Federal Gov-*
11 *ernment pursuant to title XI of the National Security*
12 *Act of 1947 and the Federal department or agency*
13 *that initially received such information, any such in-*
14 *formation that forms the basis for the advisory, alert,*
15 *or warning or the source of such information;*

16 *“(2) information that is proprietary, business*
17 *sensitive, relates specifically to the submitting person*
18 *or entity, or is otherwise not appropriate for disclo-*
19 *sure in the public domain; and*

20 *“(3) any information that is restricted by stat-*
21 *ute, rule, or regulation, including information re-*
22 *stricted from disclosure under title XI of the National*
23 *Security Act of 1947, and information relating to*
24 *sources and methods and the national security of the*
25 *United States.*

1 **“SEC. 248. DEFINITIONS.**

2 *“In this subtitle:*

3 *“(1) CYBER THREAT INFORMATION.—The term*
4 *‘cyber threat information’ means the information di-*
5 *rectly pertaining to a vulnerability of, or threat to,*
6 *a system or network of a government or private enti-*
7 *ty, including information pertaining to the protection*
8 *of a system or network from—*

9 *“(A) efforts to degrade, disrupt, or destroy*
10 *such system or network; or*

11 *“(B) efforts to gain unauthorized access to*
12 *a system or network, including efforts to gain*
13 *such unauthorized access to steal or misappro-*
14 *priate private or government information.*

15 *“(2) CYBERSECURITY THREAT.—The term ‘cy-*
16 *bersecurity threat’ means a vulnerability of, or threat*
17 *to, a system or network of a government or private*
18 *entity, including—*

19 *“(A) efforts to degrade, disrupt, or destroy*
20 *such system or network; or*

21 *“(B) efforts to gain unauthorized access to*
22 *a system or network, including efforts to gain*
23 *such unauthorized access to steal or misappro-*
24 *priate private or government information.*

25 **“SEC. 249. SAVINGS CLAUSE.**

26 *“Nothing in this subtitle shall be interpreted to—*

1 “(1) alter or amend the authorities of any Fed-
2 eral department or agency other than the Department
3 of Homeland Security, including the law enforcement
4 or intelligence authorities of any such Federal depart-
5 ment or agency or the authority of any such Federal
6 department or agency to protect sources and methods
7 and the national security;

8 “(2) limit or modify an existing information
9 sharing or other relationship;

10 “(3) prohibit a new information sharing or other
11 relationship;

12 “(4) require a new information sharing or other
13 relationship between the Federal Government and a
14 private sector entity;

15 “(5) alter or otherwise limit the authority of any
16 Federal department or agency to also undertake any
17 activities that the Department of Homeland Security
18 is authorized to undertake pursuant to this section; or

19 “(6) provide additional authority to, or modify
20 an existing authority of the Department of Homeland
21 Security to control, modify, require, or otherwise di-
22 rect the cybersecurity efforts of a private-sector entity
23 or a component of the Federal Government or a State,
24 local, or tribal government.”.

1 (2) *CLERICAL AMENDMENT.*—*The table of con-*
 2 *tents in section 1(b) of such Act, as amended by sec-*
 3 *tion 2, is further amended by adding at the end of*
 4 *the items relating to title II the following new items:*

*“Subtitle E—Department of Homeland Security Cybersecurity Information
 Sharing*

“Sec. 241. Information sharing.

“Sec. 242. Establishment of National Cybersecurity and Communications Inte-
gration Center.

“Sec. 243. Board of advisors.

“Sec. 244. Charter.

“Sec. 245. Participation.

“Sec. 246. Annual report.

“Sec. 247. Authority to issue warnings.

“Sec. 248. Definitions.

“Sec. 249. Savings clause.”.

5 **(b) AUTHORIZATION OF APPROPRIATION FOR THE NA-**
 6 **TIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRA-**
 7 **TION CENTER.**—*There is authorized to be appropriated*
 8 *\$4,000,000 for each of fiscal years 2013, 2014, and 2015*
 9 *for the administration and management of the National*
 10 *Cybersecurity and Communications Integration Center.*

11 **SEC. 4. CYBERSECURITY RESEARCH AND DEVELOPMENT.**

12 **(a) IN GENERAL.**—*Title III of the Homeland Security*
 13 *Act of 2002 is amended by adding at the end the following:*

14 **“SEC. 318. CYBERSECURITY RESEARCH AND DEVELOPMENT.**

15 **“(a) IN GENERAL.**—*The Under Secretary for Science*
 16 *and Technology shall support research, development, test-*
 17 *ing, evaluation, and transition of cybersecurity technology.*
 18 *Such support shall include fundamental, long-term research*
 19 *to improve the ability of the United States to prevent, pro-*

1 *tect against, detect, respond to, and recover from acts of*
2 *terrorism and cyber attacks, with an emphasis on research*
3 *and development relevant to attacks that would cause a de-*
4 *bitating impact on national security, national economic*
5 *security, or national public health and safety.*

6 “(b) *ACTIVITIES.*—*The research and development test-*
7 *ing, evaluation, and transition supported under subsection*
8 *(a) shall include work to—*

9 “(1) *advance the development and accelerate the*
10 *deployment of more secure versions of fundamental*
11 *Internet protocols and architectures, including for the*
12 *domain name system and routing protocols;*

13 “(2) *improve, create, and advance the research*
14 *and development of techniques and technologies for*
15 *proactive detection and identification of threats, at-*
16 *tacks, and acts of terrorism before they occur;*

17 “(3) *advance technologies for detecting attacks or*
18 *intrusions, including real-time monitoring and real-*
19 *time analytic technologies;*

20 “(4) *improve and create mitigation and recovery*
21 *methodologies, including techniques and policies for*
22 *real-time containment of attacks and development of*
23 *resilient networks and systems;*

24 “(5) *develop and support infrastructure and*
25 *tools to support cybersecurity research and develop-*

1 *ment efforts, including modeling, test beds, and data*
2 *sets for assessment of new cybersecurity technologies;*

3 *“(6) assist in the development and support of*
4 *technologies to reduce vulnerabilities in process con-*
5 *trol systems;*

6 *“(7) develop and support cyber forensics and at-*
7 *tack attribution;*

8 *“(8) test, evaluate, and facilitate the transfer of*
9 *technologies associated with the engineering of less*
10 *vulnerable software and securing the information*
11 *technology software development lifecycle;*

12 *“(9) ensure new cybersecurity technology is sci-*
13 *entifically and operationally validated; and*

14 *“(10) facilitate the planning, development, and*
15 *implementation of international cooperative activities*
16 *(as defined in section 317) to address cybersecurity*
17 *and energy infrastructure with foreign public or pri-*
18 *vate entities, governmental organizations, businesses*
19 *(including small business concerns and social and*
20 *economically disadvantaged small business concerns*
21 *(as those terms are defined in sections 3 and 8 of the*
22 *Small Business Act (15 U.S.C. 632 and 637) respec-*
23 *tively)), federally funded research and development*
24 *centers and universities from countries that may in-*
25 *clude Israel, the United Kingdom, Canada, Australia,*

1 *Singapore, Germany, New Zealand, and other allies,*
2 *as determined by the Secretary, in research and devel-*
3 *opment of technologies, best practices, and other*
4 *means to protect critical infrastructure, including the*
5 *national electric grid.*

6 “(c) *COORDINATION.*—*In carrying out this section, the*
7 *Under Secretary shall coordinate all activities with—*

8 “(1) *the Under Secretary for National Protection*
9 *and Programs Directorate; and*

10 “(2) *the heads of other relevant Federal depart-*
11 *ments and agencies, including the National Science*
12 *Foundation, the Defense Advanced Research Projects*
13 *Agency, the Information Assurance Directorate of the*
14 *National Security Agency, the National Institute of*
15 *Standards and Technology, the Department of Com-*
16 *merce, academic institutions, the Networking and In-*
17 *formation Technology Research and Development Pro-*
18 *gram, and other appropriate working groups estab-*
19 *lished by the President to identify unmet needs and*
20 *cooperatively support activities, as appropriate.”.*

21 “(b) *CLERICAL AMENDMENT.*—*The table of contents in*
22 *section 1(b) of such Act, as amended by sections 2 and 3,*
23 *is further amended by inserting after the item relating to*
24 *section 317 the following new item:*

 “*Sec. 318. Cybersecurity research and development.*”.

1 **SEC. 5. REPORT ON SUPPORT FOR REGIONAL CYBERSECURITY COOPERATIVES.**
2

3 (a) *IN GENERAL.*—Not later than 180 days after the
4 date of the enactment of this Act, the Secretary of Homeland
5 Security shall submit to the Committee on Homeland Security
6 of the House of Representatives and the Committee on
7 Homeland Security and Governmental Affairs of the Senate
8 a report on what support, if any, the Department of Home-
9 land Security might provide to regional, State, and local
10 grassroots cyber cooperatives.

11 (b) *CONTENTS.*—The report shall include an analysis
12 of the progress in establishing the “NET Guard” authorized
13 under section 224 of the Homeland Security Act of 2002
14 (6 U.S.C. 144) to build a national technology guard for
15 cyber response capabilities and an assessment of whether
16 a grant process for pilot regional, State, or local cyber co-
17 operatives would be beneficial. Such assessment should—

18 (1) evaluate whether the grant process should in-
19 clude a methodology of identifying recognized na-
20 tional experts in relevant areas of science and tech-
21 nology, including agreed upon metrics measuring the
22 expertise and demonstrated capabilities of such ex-
23 perts; and

24 (2) address the following:

25 (A) The appropriateness of the establish-
26 ment and maintenance of a national volunteer

1 *experts registry system comprised of the dem-*
2 *onstrated national experts described in this*
3 *paragraph, together with information relating to*
4 *their particular areas of expertise and who may*
5 *be called upon to respond to a cyber incident.*

6 *(B) The need to identify and leverage exist-*
7 *ing capabilities of cyber response and cyber*
8 *workforce challenge programs in States, local*
9 *governments, private sector entities, and non-*
10 *profit organizations to potentially accelerate the*
11 *implementation of the NET Guard.*

12 *(C) The requirements for the implementa-*
13 *tion of a plan to improve national capability*
14 *with minimum descriptions of the following:*

15 *(i) How to evaluate the demonstrated*
16 *national experts in relevant areas of science*
17 *and technology.*

18 *(ii) How to establish and maintain the*
19 *national volunteer experts registry system.*

20 *(iii) Potential funding models incor-*
21 *porating private sector funding.*

1 **SEC. 6. CYBERSECURITY DOMESTIC PREPAREDNESS CON-**
2 **SORTIUM AND CYBERSECURITY TRAINING**
3 **CENTER.**

4 (a) *CYBERSECURITY DOMESTIC PREPAREDNESS CON-*
5 *SORTIUM.*—

6 (1) *IN GENERAL.*—*The Secretary of Homeland*
7 *Security may establish a consortium to be known as*
8 *the “Cybersecurity Domestic Preparedness Consor-*
9 *tium”.*

10 (2) *FUNCTIONS.*—*The Consortium established*
11 *under paragraph (1) may—*

12 (A) *provide training to State and local first*
13 *responders and officials specifically for pre-*
14 *paring and responding to cybersecurity attacks;*

15 (B) *develop and update a curriculum uti-*
16 *lizing the DHS National Cyber Security Divi-*
17 *sion sponsored Community Cyber Security Ma-*
18 *turity Model (CCSMM) for State and local first*
19 *responders and officials;*

20 (C) *provide technical assistance services to*
21 *build and sustain capabilities in support of cy-*
22 *bersecurity preparedness and response; and*

23 (D) *conduct cybersecurity training and*
24 *simulation exercises to defend from and respond*
25 *to cyber attacks.*

1 (3) *MEMBERS.*—*The Consortium shall consist of*
2 *academic, nonprofit, and government partners that*
3 *develop, update, and deliver cybersecurity training in*
4 *support of homeland security.*

5 (b) *CYBERSECURITY TRAINING CENTER.*—*As a part of*
6 *the Cybersecurity Domestic Preparedness Consortium, the*
7 *Secretary may establish where appropriate one or more cy-*
8 *bersecurity training centers to provide training courses and*
9 *other resources for State and local first responders and offi-*
10 *cial to improve preparedness and response capabilities.*

11 (c) *PLAN FOR FUSION CENTERS.*—*The Cybersecurity*
12 *Domestic Preparedness Consortium shall develop a plan to*
13 *implement as one of the Cybersecurity Training Centers a*
14 *one-year voluntary pilot program to test and assess the fea-*
15 *sibility, costs, and benefits of providing cybersecurity train-*
16 *ing to State and local law enforcement personnel through*
17 *the national network of fusion centers.*

18 (d) *PILOT PROGRAM.*—

19 (1) *IN GENERAL.*—*Not later than one year after*
20 *the date of the enactment of the Act, the Secretary*
21 *shall implement a one-year voluntary pilot program*
22 *to train State and local law enforcement personnel in*
23 *the national network of fusion centers in cyber secu-*
24 *rity standards, procedures, and best practices.*

1 (2) *CURRICULUM AND PERSONNEL.*—*In creating*
2 *the curriculum for the training program and con-*
3 *ducting the program, the Secretary may assign per-*
4 *sonnel from the Department of Homeland Security,*
5 *including personnel from the Office of Cybersecurity*
6 *and Communications.*

7 (3) *COORDINATION.*—*The curriculum for the*
8 *training and for conducting the program will be co-*
9 *ordinated with that of the Cyber Security Domestic*
10 *Preparedness Consortium.*

11 **SEC. 7. SAVINGS CLAUSE.**

12 *Nothing in this Act shall be interpreted to—*

13 (1) *alter or amend the authorities of any Federal*
14 *department or agency other than the Department of*
15 *Homeland Security, including the law enforcement or*
16 *intelligence authorities of any such Federal depart-*
17 *ment or agency or the authority of any such Federal*
18 *department or agency to protect sources and methods*
19 *and the national security;*

20 (2) *alter or otherwise limit the authority of any*
21 *Federal department or agency to also undertake any*
22 *activities that the Department of Homeland Security*
23 *is authorized to undertake pursuant to this section; or*

24 (3) *provide additional authority to, or modify*
25 *an existing authority of the Department of Homeland*

1 *Security to control, modify, require, or otherwise di-*
2 *rect the cybersecurity efforts of a private-sector entity*
3 *or a component of the Federal Government or a State,*
4 *local, or tribal government.*

Union Calendar No. 501

112TH CONGRESS
2^D SESSION

H. R. 3674

[Report No. 112-592, Part I]

A BILL

To amend the Homeland Security Act of 2002 to make certain improvements in the laws relating to cybersecurity, and for other purposes.

SEPTEMBER 21, 2012

The Committee on Energy and Commerce discharged; committed to the Committee of the Whole House on the State of the Union and ordered to be printed