

**AMENDMENT IN THE NATURE OF A SUBSTITUTE  
TO H.R. 3674  
OFFERED BY MR. DANIEL E. LUNGREN OF  
CALIFORNIA**

Strike all after the enacting clause and insert the following:

**1 SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Promoting and En-  
3 hancing Cybersecurity and Information Sharing Effective-  
4 ness Act of 2012” or the “PRECISE Act of 2012”.

**5 SEC. 2. DEPARTMENT OF HOMELAND SECURITY  
6 CYBERSECURITY ACTIVITIES.**

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

**10 “SEC. 226. DEPARTMENT OF HOMELAND SECURITY  
11 CYBERSECURITY ACTIVITIES.**

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

1           “(1) conduct risk assessments, subject to the  
2           availability of resources and, solely upon request  
3           from critical infrastructure owners and operators,  
4           critical infrastructure information systems;

5           “(2) assist in fostering the development, in con-  
6           junction with the National Institute of Standards  
7           and Technology and other Federal departments and  
8           agencies and the private sector, of essential informa-  
9           tion security technologies and capabilities for pro-  
10          tecting Federal systems and critical infrastructure  
11          information systems, including comprehensive pro-  
12          tective capabilities and other technological solutions;

13          “(3) assist in efforts to mitigate communica-  
14          tions and information technology supply chain  
15          vulnerabilities;

16          “(4) support nationwide awareness and out-  
17          reach efforts, to include participation in appropriate  
18          interagency cybersecurity awareness and education  
19          programs, to educate the public.

20          “(5) conduct exercises, simulations, and other  
21          activities designed to support and evaluate the na-  
22          tional cyber incident response plan; and

23          “(6) subject to the availability of resources and,  
24          upon request of critical infrastructure owners and  
25          operators, provide technical assistance, including

1        sending on-site teams, to such critical infrastructure  
2        owners and operators.

3        “(b) INTERAGENCY DUTIES.—At the direction of the  
4        Office of Management and Budget pursuant to subchapter  
5        II of chapter 35 of title 44, United States Code, the Sec-  
6        retary shall—

7                “(1) conduct targeted risk assessments and  
8                operational evaluations, in conjunction with the  
9                heads of other agencies, for Federal systems that  
10              may include threat, vulnerability, and impact assess-  
11              ments and penetration testing;

12              “(2) in conjunction with the National Institute  
13              of Standards and Technology and appropriate Fed-  
14              eral departments and agencies, as well as the private  
15              sector, provide for the use of consolidated intrusion  
16              detection, prevention, or other protective capabilities  
17              and use associated countermeasures for the purpose  
18              of protecting Federal systems from cybersecurity  
19              threats;

20              “(3) in conjunction with other agencies and the  
21              private sector, assess and foster the development of  
22              information security technologies and capabilities for  
23              use and dissemination throughout the Department  
24              of Homeland Security and to be made available  
25              across multiple agencies;

1           “(4) designate an entity within the Department  
2 of Homeland Security to receive reports and infor-  
3 mation about cybersecurity incidents, threats, and  
4 vulnerabilities affecting Federal systems; and

5           “(5) provide incident detection, analysis, miti-  
6 gation, and response information and remote or on-  
7 site technical assistance for Federal systems.

8           “(c) COORDINATION.—

9           “(1) COORDINATION WITH OTHER ENTITIES.—

10 In carrying out cybersecurity activities subsection  
11 (a), the Secretary shall coordinate, as appropriate,  
12 with—

13           “(A) the head of relevant Federal depart-  
14 ments or agencies;

15           “(B) representatives of State and local  
16 governments;

17           “(C) owners and operators of critical infra-  
18 structure;

19           “(D) suppliers of technology for owners  
20 and operators of critical infrastructure;

21           “(E) academia; and

22           “(F) international organizations and for-  
23 eign partners.

24           “(2) LEAD DHS CYBERSECURITY OFFICIAL.—

25 The Secretary shall designate a lead cybersecurity

1 official within the Department to provide leadership  
2 to the cybersecurity activities of the Department and  
3 to ensure that the Department's cybersecurity activi-  
4 ties under this subtitle are coordinated with all other  
5 infrastructure protection and cyber-related programs  
6 and activities of the Department, including those of  
7 any intelligence or law enforcement components or  
8 entities within the Department.

9 “(3) REPORTS TO CONGRESS.—The lead DHS  
10 cybersecurity official shall make annual reports to  
11 the appropriate committees of Congress on the co-  
12 ordination of cyber-related programs across the De-  
13 partment.

14 “(d) STRATEGY.—In carrying out the cybersecurity  
15 activities of the Department under subsection (a), the Sec-  
16 retary shall develop and maintain a strategy that—

17 “(1) articulates the actions of the Department  
18 that are necessary to assure the readiness, reli-  
19 ability, continuity, integrity, and resilience of Fed-  
20 eral systems and critical infrastructure information  
21 systems;

22 “(2) includes explicit goals and objectives for  
23 the Department as well as specific timeframes for  
24 achievement of stated goals and objectives by the  
25 Department;

1           “(3) fosters the continued superiority and reli-  
2           ability of the United States information technology  
3           and communications sectors; and

4           “(4) ensures that activities of the Department  
5           are undertaken in a manner that protects statutory  
6           privacy rights and civil liberties of United States  
7           persons.

8           “(e) NO RIGHT OR BENEFIT.—The provision of as-  
9           sistance or information to critical infrastructure owners  
10          and operators, upon request of such critical infrastructure  
11          owners and operators, under this section shall be at the  
12          discretion of the Secretary and subject to the availability  
13          of resources. The provision of certain assistance or infor-  
14          mation to one critical infrastructure owner or and oper-  
15          ator pursuant to this section shall not create a right or  
16          benefit, substantive or procedural, to similar assistance or  
17          information for any other critical infrastructure owner or  
18          and operator.

19          “(f) SAVINGS CLAUSE.—Nothing in this subtitle shall  
20          be interpreted to—

21                 “(1) alter or amend the authorities of any Fed-  
22                 eral department or agency other than the Depart-  
23                 ment of Homeland Security, including the law en-  
24                 forcement or intelligence authorities of any such  
25                 Federal department or agency or the authority of

1 any such Federal department or agency to protect  
2 sources and methods and the national security;

3 “(2) limit or modify an existing information  
4 sharing or other relationship;

5 “(3) prohibit a new information sharing or  
6 other relationship;

7 “(4) require a new information sharing or other  
8 relationship between the Federal Government and a  
9 private sector entity;

10 “(5) alter or otherwise limit the authority of  
11 any Federal department or agency to also undertake  
12 any activities that the Department of Homeland Se-  
13 curity is authorized to undertake pursuant to this  
14 section; or

15 “(6) provide additional authority to, or modify  
16 an existing authority of the Department of Home-  
17 land Security to control, modify, require, or other-  
18 wise direct the cybersecurity efforts of a private-sec-  
19 tor entity or a component of the Federal Govern-  
20 ment or a State, local, or tribal government.

21 “(g) DEFINITIONS.—In this section:

22 “(1) The term ‘Federal systems’ means infor-  
23 mation systems owned, operated, leased, or other-  
24 wise controlled by a Federal department or agency,  
25 or on behalf of a Federal department or agency, ex-

1       cept for national security systems or those informa-  
2       tion systems under the control of, used by, or stor-  
3       ing information of the Department of Defense or  
4       any element of the Intelligence Community, includ-  
5       ing any information systems used or operated by a  
6       contractor of the Department of Defense or any ele-  
7       ment of the Intelligence Community, or other orga-  
8       nization on behalf of the Department of Defense or  
9       any element of the Intelligence Community.

10           “(2) The term ‘critical infrastructure informa-  
11       tion systems’ means any information system that  
12       is—

13                   “(A) vital to the functioning of critical in-  
14       frastructure as defined in section 5195c(e) of  
15       title 42, United States Code; or

16                   “(B) owned or operated by or on behalf of  
17       a State or local government entity that is nec-  
18       essary to ensure essential government oper-  
19       ations continue.

20           “(3) The term ‘information system’ means any  
21       equipment or interconnected system or subsystem of  
22       equipment that is used in the automatic acquisition,  
23       storage, manipulation, management, movement, con-  
24       trol, display, switching, interchange, transmission, or  
25       reception of data or information, and includes—

1 “(A) computers and computer networks;

2 “(B) ancillary equipment;

3 “(C) software, firmware, and related proce-  
4 dures;

5 “(D) services, including support services;

6 and

7 “(E) related resources.

8 “(4) The term ‘national security system’ means  
9 any information infrastructure (including any tele-  
10 communications system) used or operated by an  
11 agency, by a contractor of an agency, or by another  
12 organization on behalf of an agency—

13 “(A) the function, operation, or use of  
14 which—

15 “(i) involves intelligence activities or  
16 intelligence-related activities;

17 “(ii) involves cryptologic activities re-  
18 lated to national security;

19 “(iii) involves command and control of  
20 military forces;

21 “(iv) involves equipment that is an in-  
22 tegral part of a weapon or weapons sys-  
23 tem; or

24 “(v) is critical to the direct fulfillment  
25 of military or intelligence missions;

1           “(B) that contains information related to  
2           the activities and other matters set forth in  
3           subparagraph (A); or

4           “(C) that is protected by procedures estab-  
5           lished for classified, national security, foreign  
6           policy, intelligence or intelligence-related, or  
7           other appropriate information.

8   **“SEC. 227. PERSONNEL AUTHORITIES RELATED TO THE OF-**  
9                   **FICE OF CYBERSECURITY AND COMMUNICA-**  
10                   **TIONS.**

11       “(a) IN GENERAL.—In order to assure that the De-  
12       partment has the necessary resources to carry out the mis-  
13       sion set forth in section 226, the Secretary may, as nec-  
14       essary, convert competitive service positions, and the in-  
15       cumbents of such positions, within the Office of  
16       Cybersecurity and Communications to excepted service, or  
17       may establish new positions within the Office of  
18       Cybersecurity and Communications in the excepted serv-  
19       ice, to the extent that the Secretary determines such posi-  
20       tions are necessary to carry out the cybersecurity func-  
21       tions of the Department.

22       “(b) COMPENSATION.—The Secretary may—

23           “(1) fix the compensation of individuals who  
24           serve in positions referred to in subsection (a) in re-  
25           lation to the rates of pay provided for comparable

1 positions in the Department and subject to the same  
2 limitations on maximum rates of pay established for  
3 employees of the Department by law or regulations;  
4 and

5 “(2) provide additional forms of compensation,  
6 including benefits, incentives, and allowances, that  
7 are consistent with and not in excess of the level au-  
8 thorized for comparable positions authorized under  
9 title 5, United States Code.

10 “(c) RETENTION BONUSES.—Notwithstanding any  
11 other provision of law, the Secretary may pay a retention  
12 bonus to any employee appointed under this section, if the  
13 Secretary determines that the bonus is needed to retain  
14 essential personnel. Before announcing the payment of a  
15 bonus under this subsection, the Secretary shall submit  
16 a written explanation of such determination to the Com-  
17 mittee on Homeland Security of the House of Representa-  
18 tives and the Committee on Homeland Security and Gov-  
19 ernmental Affairs of the Senate.

20 “(d) ANNUAL REPORT.—Not later than one year  
21 after the date of the enactment of this section, and annu-  
22 ally thereafter, the Secretary shall submit to appropriate  
23 Congressional committees a detailed report that includes,  
24 for the period covered by the report—

1           “(1) a discussion the Secretary’s use of the  
2 flexible authority authorized under this section to re-  
3 cruit and retain qualified employees;

4           “(2) metrics on relevant personnel actions, in-  
5 cluding—

6           “(A) the number of qualified employees  
7 hired by occupation and grade, level, or pay  
8 band;

9           “(B) the total number of veterans hired;

10           “(C) the number of separations of qualified  
11 employees;

12           “(D) the number of retirements of quali-  
13 fied employees; and

14           “(E) the number and amounts of recruit-  
15 ment, relocation, and retention incentives paid  
16 to qualified employees by occupation and grade,  
17 level, or pay band; and

18           “(3) long-term and short-term strategic goals to  
19 address critical skills deficiencies, including an anal-  
20 ysis of the numbers of and reasons for attrition of  
21 employees and barriers to recruiting and hiring indi-  
22 viduals qualified in cybersecurity.”.

23           (b) CLERICAL AMENDMENT.—The table of contents  
24 in section 2(b) of such Act is amended by inserting after  
25 the 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 Communications.”.

1           (c) **PLAN FOR EXECUTION OF AUTHORITIES.**—Not  
2 later than 120 days after the date of the enactment of  
3 this Act, the Secretary of Homeland Security shall submit  
4 to the Committee on Homeland Security of the House of  
5 Representatives and the Committee on Homeland Security  
6 and Governmental Affairs of the Senate a report con-  
7 taining a plan for the execution of the authorities con-  
8 tained in the amendment made by subsection (a).

9   **SEC. 3. DEPARTMENT OF HOMELAND SECURITY**  
10                                   **CYBERSECURITY INFORMATION SHARING.**

11           (a) **DEPARTMENT OF HOMELAND SECURITY**  
12 **CYBERSECURITY INFORMATION SHARING.**—

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

16   **“Subtitle E—Department of Home-**  
17   **land Security Cybersecurity In-**  
18   **formation Sharing**

19   **“SEC. 241. INFORMATION SHARING.**

20           “The Secretary shall make appropriate cyber threat  
21 information obtained by the Department or other informa-  
22 tion appropriately in the possession of the Department  
23 available to appropriate owners and operators of critical  
24 infrastructure on a timely basis consistent with the statu-

1 tory and other appropriate restrictions on the dissemina-  
2 tion of such information and with the responsibilities of  
3 the Secretary under this title.

4 **“SEC. 242. ESTABLISHMENT OF NATIONAL CYBERSECURITY**  
5 **AND COMMUNICATIONS INTEGRATION CEN-**  
6 **TER.**

7 “(a) ESTABLISHMENT.—There is established within  
8 the Department the National Cybersecurity and Commu-  
9 nications Integration Center.

10 “(b) PURPOSE.—The center established pursuant to  
11 subsection (a) shall be the primary entity within the De-  
12 partment for sharing timely cyber threat information and  
13 exchanging technical assistance, advice, and support with  
14 appropriate entities pursuant to the Department’s au-  
15 thorities.

16 **“SEC. 243. BOARD OF ADVISORS.**

17 “(a) IN GENERAL.—The National Cybersecurity and  
18 Communications Integration Center shall have a board of  
19 advisors which shall advise the Secretary on the efficient  
20 operation of the National Cybersecurity and Communica-  
21 tions Integration Center.

22 “(b) COMPOSITION.—The board shall be composed of  
23 13 members, including the following:

24 “(1) Ten representatives from the critical infra-  
25 structure sectors enumerated in the National Infra-

1 structure Protection Plan, of which at least one  
2 member shall represent a small business interest and  
3 at least one member shall represent each of the fol-  
4 lowing sectors:

5 “(A) Banking and finance.

6 “(B) Communications.

7 “(C) Defense industrial base.

8 “(D) Energy, electricity subsector.

9 “(E) Energy, oil, and natural gas sub-  
10 sector.

11 “(F) Health care and public health.

12 “(G) Information technology.

13 “(H) Water.

14 “(2) Two representatives from the privacy and  
15 civil liberties community.

16 “(3) The Chair of the National Council of In-  
17 formation Sharing and Analysis Centers.

18 “(c) INITIAL APPOINTMENT.—Not later than 30 days  
19 after the date of the enactment of this subtitle, the Sec-  
20 retary of Homeland Security, in consultation with the  
21 heads of the sector specific agencies of the critical infra-  
22 structure sectors enumerated in the National Infrastruc-  
23 ture Protection Plan, shall appoint the members of the  
24 board described under subsection (b) from individuals  
25 identified by the sector coordinating councils of the critical

1 infrastructure sectors enumerated in the National Infra-  
2 structure Protection Plan.

3 “(d) TERMS.—

4 “(1) CRITICAL INFRASTRUCTURE REPRESENTA-  
5 TIVES.—Each member of the board described in  
6 subsection (b)(1) shall be appointed for a term that  
7 is not less than one year and not longer than three  
8 years from the date of the member’s appointment,  
9 as determined by the member’s sector coordinating  
10 council.

11 “(2) OTHER REPRESENTATIVES.—Each mem-  
12 ber of the board described in subsection (b)(2) or (3)  
13 shall serve an initial term that is not less than two  
14 years and not longer than three years from the date  
15 of the member’s appointment, and each such mem-  
16 ber shall select the member’s successor.

17 “(e) DUTIES.—The board shall—

18 “(1) meet not less frequently than quarterly;

19 “(2) act as an advocate on behalf of the private  
20 sector in improving the operations of the National  
21 Cybersecurity Communications Integration Center;  
22 and

23 “(3) submit to the Secretary and the appro-  
24 priate committees of Congress the annual report de-  
25 scribed in section 247.

1           “(f) ACCESS TO INFORMATION.—The members of the  
2 board shall, subject to the laws and procedures applicable  
3 to national security background investigations and secu-  
4 rity clearances, be provided with the appropriate security  
5 clearances and have access to appropriate information  
6 shared with the National Cybersecurity and Communica-  
7 tions Integration Center and shall be subject to all of the  
8 limitations on the use of such information.

9           “(g) SUB-BOARDS.—The board shall have the author-  
10 ity to constitute such sub-boards, or other advisory groups  
11 or panels, as may be necessary to assist the board in car-  
12 rying out its functions under this section.

13 **“SEC. 244. CHARTER.**

14           “The Secretary shall develop a charter to govern the  
15 operations and administration of the National  
16 Cybersecurity and Communications Integration Center.  
17 The charter shall include each of the following:

18                   “(1) The organizational structure of the Na-  
19 tional Cybersecurity and Communications Integra-  
20 tion Center, including a delineation of the mission  
21 expectations and responsibilities of the various ele-  
22 ments assigned to the Center.

23                   “(2) A mission statement of the National  
24 Cybersecurity and Communications Integration Cen-  
25 ter.

1           “(3) A plan that promotes broad participation  
2           by large, medium, and small business owners and  
3           operators of networks or systems in the private sec-  
4           tor, entities operating critical infrastructure, edu-  
5           cational institutions, State, tribal, and local govern-  
6           ments, and the Federal Government.

7           “(4) Procedures for making appropriate cyber  
8           incident information available to outside groups for  
9           academic research and insurance actuarial purposes.

10 **“SEC. 245. PARTICIPATION.**

11           “Not later than 90 days after the date of the enact-  
12           ment of this subtitle, the Secretary shall publish the cri-  
13           teria and procedures for voluntary participation and vol-  
14           untary physical collocation by appropriate Federal, State  
15           and local government departments, agencies and entities,  
16           and private sector businesses and organizations within the  
17           National Cybersecurity and Communications Integration  
18           Center.

19 **“SEC. 246. ANNUAL REPORT.**

20           ““The board of advisors of the National Cybersecurity  
21           Communications Integration Center shall submit to the  
22           Secretary and the appropriate committees of Congress an  
23           annual report on the status of the National Cybersecurity  
24           Communications Integration Center and how the Center  
25           accomplished its purpose under section 242 during the

1 year covered by the report. Each such report shall include,  
2 for the year covered by the report—

3 “(1) information on the amount and nature of  
4 information shared by and through the Center;

5 “(2) the number of violations of statutory infor-  
6 mation sharing restrictions and the procedures es-  
7 tablished for the Center and any steps taken by the  
8 Center to reduce and eliminate such violations;

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

11 “(4) proposed ways to improve information  
12 sharing by and through the Center.

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

14 “The Secretary may, in coordination with appropriate  
15 Federal departments and agencies, provide advisories,  
16 alerts, and warnings to relevant companies, targeted sec-  
17 tors, other government entities, or the general public re-  
18 garding potential cybersecurity threats as appropriate. In  
19 issuing such an advisory, alert, or warning, the Secretary  
20 shall not disclose—

21 “(1) without the express consent of an entity  
22 voluntarily sharing information with the Federal  
23 Government and the Federal department or agency  
24 that initially received such information, any such in-

1 formation that forms the basis for the advisory,  
2 alert, or warning or the source of such information;

3 “(2) information that is proprietary, business  
4 sensitive, relates specifically to the submitting per-  
5 son or entity, or is otherwise not appropriate for dis-  
6 closure in the public domain; and

7 “(3) any information that is restricted by stat-  
8 ute, rule, or regulation, and information relating to  
9 sources and methods and the national security of the  
10 United States.

11 **“SEC. 248. DEFINITIONS.**

12 “In this subtitle:

13 “(1) CYBER THREAT INFORMATION.—The term  
14 ‘cyber threat information’ means the information di-  
15 rectly pertaining to a vulnerability of, or threat to,  
16 a system or network of a government or private enti-  
17 ty, including information pertaining to the protection  
18 of a system or network from—

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.

1           “(2) CYBERSECURITY THREAT.—The term  
2           ‘cybersecurity threat’ means a vulnerability of, or  
3           threat to, a system or network of a government or  
4           private entity, including—

5                   “(A) efforts to degrade, disrupt, or destroy  
6                   such system or network; or

7                   “(B) efforts to gain unauthorized access to  
8                   a system or network, including efforts to gain  
9                   such unauthorized access to steal or misappro-  
10                  priate private or government information.

11 **“SEC. 249. SAVINGS CLAUSE.**

12           “Nothing in this subtitle shall be interpreted to—

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

20                   “(2) limit or modify an existing information  
21                   sharing or other relationship;

22                   “(3) prohibit a new information sharing or  
23                   other relationship;

1           “(4) require a new information sharing or other  
2 relationship between the Federal Government and a  
3 private sector entity;

4           “(5) alter or otherwise limit the authority of  
5 any Federal department or agency to also undertake  
6 any activities that the Department of Homeland Se-  
7 curity is authorized to undertake pursuant to this  
8 section; or

9           “(6) provide additional authority to, or modify  
10 an existing authority of the Department of Home-  
11 land Security to control, modify, require, or other-  
12 wise direct the cybersecurity efforts of a private-sec-  
13 tor entity or a component of the Federal Govern-  
14 ment or a State, local, or tribal government.”.

15           (2) CLERICAL AMENDMENT.—The table of con-  
16 tents in section 2(b) of such Act, as amended by sec-  
17 tion 2, is further amended by adding at the end of  
18 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.”.

1 (b) AUTHORIZATION OF APPROPRIATION FOR THE  
2 NATIONAL CYBERSECURITY AND COMMUNICATIONS INTE-  
3 GRATION CENTER.—There is authorized to be appro-  
4 priated \$4,000,000 for each of fiscal years 2013, 2014,  
5 and 2015 for the administration and management of the  
6 National Cybersecurity and Communications Integration  
7 Center.

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

9 (a) IN GENERAL.—Title III of the Homeland Secu-  
10 rity Act of 2002 is amended by adding at the end the fol-  
11 lowing:

12 **“SEC. 318. CYBERSECURITY RESEARCH AND DEVELOP-**  
13 **MENT.**

14 “(a) IN GENERAL.—The Under Secretary for Science  
15 and Technology shall support research, development, test-  
16 ing, evaluation, and transition of cybersecurity technology.  
17 Such support shall include fundamental, long-term re-  
18 search to improve the ability of the United States to pre-  
19 vent, protect against, detect, respond to, and recover from  
20 acts of terrorism and cyber attacks, with an emphasis on  
21 research and development relevant to attacks that would  
22 cause a debilitating impact on national security, national  
23 economic security, or national public health and safety.

1       “(b) ACTIVITIES.—The research and development  
2 testing, evaluation, and transition supported under sub-  
3 section (a) shall include work to—

4           “(1) advance the development and accelerate  
5 the deployment of more secure versions of funda-  
6 mental Internet protocols and architectures, includ-  
7 ing for the domain name system and routing proto-  
8 cols;

9           “(2) improve, create, and advance the research  
10 and development of techniques and technologies for  
11 proactive detection and identification of threats, at-  
12 tacks, and acts of terrorism before they occur;

13           “(3) advance technologies for detecting attacks  
14 or intrusions, including real-time monitoring and  
15 real-time analytic technologies;

16           “(4) improve and create mitigation and recov-  
17 ery methodologies, including techniques and policies  
18 for real-time containment of attacks and develop-  
19 ment of resilient networks and systems;

20           “(5) develop and support infrastructure and  
21 tools to support cybersecurity research and develop-  
22 ment efforts, including modeling, test beds, and data  
23 sets for assessment of new cybersecurity tech-  
24 nologies;

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

4           “(7) develop and support cyber forensics and  
5 attack attribution;

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

10          “(9) ensure new cybersecurity technology is sci-  
11 entifically and operationally validated; and

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

1 search and development of technologies, best prac-  
2 tices, and other means to protect critical infrastruc-  
3 ture, including the national electric grid.

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

6 “(1) the Under Secretary for National Protec-  
7 tion and Programs Directorate; and

8 “(2) the heads of other relevant Federal depart-  
9 ments and agencies, including the National Science  
10 Foundation, the Defense Advanced Research  
11 Projects Agency, the Information Assurance Direc-  
12 torate of the National Security Agency, the National  
13 Institute of Standards and Technology, the Depart-  
14 ment of Commerce, academic institutions, the Net-  
15 working and Information Technology Research and  
16 Development Program, and other appropriate work-  
17 ing groups established by the President to identify  
18 unmet needs and cooperatively support activities, as  
19 appropriate.”.

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

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

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

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

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

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

25 (2) address the following:

1           (A) The appropriateness of the establish-  
2           ment and maintenance of a national volunteer  
3           experts registry system comprised of the dem-  
4           onstrated national experts described in this  
5           paragraph, together with information relating  
6           to their particular areas of expertise and who  
7           may be called upon to respond to a cyber inci-  
8           dent.

9           (B) The need to identify and leverage ex-  
10          isting capabilities of cyber response and cyber  
11          workforce challenge programs in States, local  
12          governments, private sector entities, and non-  
13          profit organizations to potentially accelerate the  
14          implementation of the NET Guard.

15          (C) The requirements for the implementa-  
16          tion of a plan to improve national capability  
17          with minimum descriptions of the following:

18                 (i) How to evaluate the demonstrated  
19                 national experts in relevant areas of  
20                 science and technology.

21                 (ii) How to establish and maintain the  
22                 national volunteer experts registry system.

23                 (iii) Potential funding models incor-  
24                 porating private sector funding.

1 **SEC. 6. REPORT ON CYBERSECURITY TRAINING FOR FU-**  
2 **SION CENTERS.**

3 The Secretary of Homeland Security shall submit a  
4 report to Congress assessing the feasibility, costs, and  
5 benefits of providing cybersecurity training to appropriate  
6 State and local personnel through the national network  
7 of fusion centers.

8 **SEC. 7. SAVINGS CLAUSE.**

9 Nothing in this Act shall be interpreted to—

10 (1) alter or amend the authorities of any Fed-  
11 eral department or agency other than the Depart-  
12 ment of Homeland Security, including the law en-  
13 forcement or intelligence authorities of any such  
14 Federal department or agency or the authority of  
15 any such Federal department or agency to protect  
16 sources and methods and the national security;

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

22 (3) provide additional authority to, or modify  
23 an existing authority of the Department of Home-  
24 land Security to control, modify, require, or other-  
25 wise direct the cybersecurity efforts of a private-sec-

- 1 tor entity or a component of the Federal Govern-
- 2 ment or a State, local, or tribal government.

