

Calendar No. 735

115TH CONGRESS
2D SESSION

S. 278

[Report No. 115-444]

To amend the Homeland Security Act of 2002 to provide for innovative research and development, and for other purposes.

IN THE SENATE OF THE UNITED STATES

FEBRUARY 2, 2017

Mr. DAINES (for himself and Mr. WARNER) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

DECEMBER 19, 2018

Reported by Mr. JOHNSON, with an amendment

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

A BILL

To amend the Homeland Security Act of 2002 to provide for innovative research and development, 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 “Support for Rapid In-
5 novation Act of 2017”.

1 **SEC. 2. CYBERSECURITY RESEARCH AND DEVELOPMENT**
2 **PROJECTS.**

3 (a) CYBERSECURITY RESEARCH AND DEVELOP-
4 MENT.—

5 (1) IN GENERAL.—Title III of the Homeland
6 Security Act of 2002 (6 U.S.C. 181 et seq.) is
7 amended by adding at the end the following new sec-
8 tion:

9 **“SEC. 321. CYBERSECURITY RESEARCH AND DEVELOP-**
10 **MENT.**

11 “(a) IN GENERAL.—The Under Secretary for Science
12 and Technology shall support the research, development,
13 testing, evaluation, and transition of cybersecurity tech-
14 nologies, including fundamental research to improve the
15 sharing of information, information security, analytics,
16 and methodologies related to cybersecurity risks and inci-
17 dents, consistent with current law.

18 “(b) ACTIVITIES.—The research and development
19 supported under subsection (a) shall serve the components
20 of the Department and shall—

21 “(1) advance the development and accelerate
22 the deployment of more secure information systems;

23 “(2) improve and create technologies for detect-
24 ing and preventing attacks or intrusions, including
25 real-time continuous diagnostics, real-time analytie

1 technologies, and full lifecycle information protec-
2 tion;

3 “(3) improve and create mitigation and recov-
4 ery methodologies, including techniques and policies
5 for real-time containment of attacks, and develop-
6 ment of resilient networks and information systems;

7 “(4) support, in coordination with non-Federal
8 entities, the review of source code that underpins
9 critical infrastructure information systems;

10 “(5) assist the development and support infra-
11 structure and tools to support cybersecurity research
12 and development efforts, including modeling,
13 testbeds, and data sets for assessment of new cyber-
14 security technologies;

15 “(6) assist the development and support of
16 technologies to reduce vulnerabilities in industrial
17 control systems;

18 “(7) assist the development and support cyber
19 forensics and attack attribution capabilities;

20 “(8) assist the development and accelerate the
21 deployment of full information lifecycle security tech-
22 nologies to enhance protection, control, and privacy
23 of information to detect and prevent cybersecurity
24 risks and incidents;

1 “(9) assist the development and accelerate the
2 deployment of information security measures, in ad-
3 dition to perimeter-based protections;

4 “(10) assist the development and accelerate the
5 deployment of technologies to detect improper infor-
6 mation access by authorized users;

7 “(11) assist the development and accelerate the
8 deployment of cryptographic technologies to protect
9 information at rest, in transit, and in use;

10 “(12) assist the development and accelerate the
11 deployment of methods to promote greater software
12 assurance;

13 “(13) assist the development and accelerate the
14 deployment of tools to securely and automatically
15 update software and firmware in use, with limited or
16 no necessary intervention by users and limited im-
17 pact on concurrently operating systems and proe-
18 cesses; and

19 “(14) assist in identifying and addressing un-
20 identified or future cybersecurity threats.

21 “(e) COORDINATION.—In carrying out this section,
22 the Under Secretary for Science and Technology shall co-
23 ordinate activities with—

24 “(1) the Under Secretary appointed pursuant to
25 section 103(a)(1)(H);

1 “(2) the heads of other relevant Federal depart-
2 ments and agencies, as appropriate; and

3 “(3) industry and academia.

4 “(d) TRANSITION TO PRACTICE.—The Under Sec-
5 retary for Science and Technology shall support projects
6 carried out under this title through the full life cycle of
7 such projects, including research, development, testing,
8 evaluation, pilots, and transitions. The Under Secretary
9 shall identify mature technologies that address existing or
10 imminent cybersecurity gaps in public or private informa-
11 tion systems and networks of information systems; protect
12 sensitive information within and outside networks of infor-
13 mation systems; identify and support necessary improve-
14 ments identified during pilot programs and testing and
15 evaluation activities; and introduce new cybersecurity
16 technologies throughout the homeland security enterprise
17 through partnerships and commercialization. The Under
18 Secretary shall target federally funded cybersecurity re-
19 search that demonstrates a high probability of successful
20 transition to the commercial market within two years and
21 that is expected to have a notable impact on the public
22 or private information systems and networks of informa-
23 tion systems.

24 “(e) DEFINITIONS.—In this section:

1 “(1) **CYBERSECURITY RISK.**—The term ‘cyber-
2 security risk’ has the meaning given such term in
3 section 227.

4 “(2) **HOMELAND SECURITY ENTERPRISE.**—The
5 term ‘homeland security enterprise’ means relevant
6 governmental and nongovernmental entities involved
7 in homeland security, including Federal, State, local,
8 and tribal government officials, private sector rep-
9 resentatives, academics, and other policy experts.

10 “(3) **INCIDENT.**—The term ‘incident’ has the
11 meaning given such term in section 227.

12 “(4) **INFORMATION SYSTEM.**—The term ‘infor-
13 mation system’ has the meaning given such term in
14 section 3502(8) of title 44, United States Code.

15 “(5) **SOFTWARE ASSURANCE.**—The term ‘soft-
16 ware assurance’ means confidence that software—

17 “(A) is free from vulnerabilities, either in-
18 tentionally designed into the software or acci-
19 dentally inserted at any time during the life
20 cycle of the software; and

21 “(B) functioning in the intended manner.”.

22 “(2) **CLERICAL AMENDMENT.**—The table of con-
23 tents in section 1(b) of the Homeland Security Act
24 of 2002 is amended by inserting after the item relat-
25 ing to the second section 319 the following new item:

“Sec. 321. Cybersecurity research and development.”.

1 (b) RESEARCH AND DEVELOPMENT PROJECTS.—
2 Section 831 of the Homeland Security Act of 2002 (6
3 U.S.C. 391) is amended—

4 (1) in subsection (a)—

5 (A) in the matter preceding paragraph (1),
6 by striking “2016” and inserting “2021”;

7 (B) in paragraph (1), by striking the last
8 sentence; and

9 (C) by adding at the end the following new
10 paragraph:

11 “(3) PRIOR APPROVAL.—In any case in which
12 the head of a component or office of the Department
13 seeks to utilize the authority under this section, such
14 head shall first receive prior approval from the Sec-
15 retary by providing to the Secretary a proposal that
16 includes the rationale for the utilization of such au-
17 thority, the funds to be spent on the use of such au-
18 thority, and the expected outcome for each project
19 that is the subject of the use of such authority. In
20 such a case, the authority for evaluating the pro-
21 posal may not be delegated by the Secretary to any-
22 one other than the Under Secretary for Manage-
23 ment.”;

24 (2) in subsection (c)—

1 (A) in paragraph (1), in the matter pre-
2 ceding subparagraph (A), by striking “2016”
3 and inserting “2021”; and

4 (B) by amending paragraph (2) to read as
5 follows:

6 “(2) REPORT.—The Secretary shall annually
7 submit to the Committee on Homeland Security and
8 the Committee on Science, Space, and Technology of
9 the House of Representatives and the Committee on
10 Homeland Security and Governmental Affairs of the
11 Senate a report detailing the projects for which the
12 authority granted by subsection (a) was utilized, the
13 rationale for such utilizations, the funds spent uti-
14 lizing such authority, the extent of cost-sharing for
15 such projects among Federal and non-Federal
16 sources, the extent to which utilization of such au-
17 thority has addressed a homeland security capability
18 gap or threat to the homeland identified by the De-
19 partment, the total amount of payments, if any, that
20 were received by the Federal Government as a result
21 of the utilization of such authority during the period
22 covered by each such report, the outcome of each
23 project for which such authority was utilized, and
24 the results of any audits of such projects.”; and

1 ~~(3)~~ by adding at the end the following new sub-
2 section:

3 ~~“(e) TRAINING.—The Secretary shall develop a train-~~
4 ~~ing program for acquisitions staff on the utilization of the~~
5 ~~authority provided under subsection (a) to ensure account-~~
6 ~~ability and effective management of projects consistent~~
7 ~~with the Program Management Improvement Account-~~
8 ~~ability Act (Public Law 114–264) and the amendments~~
9 ~~made by such Act.”.~~

10 ~~(e) NO ADDITIONAL FUNDS AUTHORIZED.—No addi-~~
11 ~~tional funds are authorized to carry out the requirements~~
12 ~~of this Act and the amendments made by this Act. Such~~
13 ~~requirements shall be carried out using amounts otherwise~~
14 ~~authorized.~~

15 **SECTION 1. SHORT TITLE.**

16 *This Act may be cited as the “Support for Rapid Inno-*
17 *vation Act of 2018”.*

18 **SEC. 2. CYBERSECURITY RESEARCH AND DEVELOPMENT**

19 **PROJECTS.**

20 ~~(a) CYBERSECURITY RESEARCH AND DEVELOP-~~
21 ~~MENT.—~~

22 ~~(1) IN GENERAL.—Title III of the Homeland Se-~~
23 ~~curity Act of 2002 (6 U.S.C. 181 et seq.) is amended~~
24 ~~by adding at the end the following:~~

1 **“SEC. 321. CYBERSECURITY RESEARCH AND DEVELOPMENT.**

2 “(a) *IN GENERAL.*—*The Under Secretary for Science*
3 *and Technology shall support the research, development,*
4 *testing, evaluation, and transition of cybersecurity tech-*
5 *nologies, including fundamental research to improve the*
6 *sharing of information, information security, analytics,*
7 *and methodologies related to cybersecurity risks and inci-*
8 *dents, consistent with current law.*

9 “(b) *ACTIVITIES.*—*The research and development sup-*
10 *ported under subsection (a) shall serve the components of*
11 *the Department and shall—*

12 “(1) *advance the development and accelerate the*
13 *deployment of more secure information systems;*

14 “(2) *improve and create technologies for detect-*
15 *ing and preventing attacks or intrusions, including*
16 *real-time continuous diagnostics, real-time analytic*
17 *technologies, and full life cycle information protection;*

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

22 “(4) *assist the development and support of infra-*
23 *structure and tools to support cybersecurity research*
24 *and development efforts, including modeling, testbeds,*
25 *and data sets for assessment of new cybersecurity*
26 *technologies;*

1 “(5) assist the development and support of tech-
2 nologies to reduce vulnerabilities in industrial control
3 systems;

4 “(6) assist the development and support of cyber
5 forensics and attack attribution capabilities;

6 “(7) assist the development and accelerate the de-
7 ployment of full information life cycle security tech-
8 nologies to enhance protection, control, and privacy of
9 information and to detect and prevent cybersecurity
10 risks and incidents;

11 “(8) assist the development and accelerate the de-
12 ployment of information security measures, in addi-
13 tion to perimeter-based protections;

14 “(9) assist the development and accelerate the de-
15 ployment of technologies to detect improper informa-
16 tion access by authorized users;

17 “(10) assist the development and accelerate the
18 deployment of cryptographic technologies to protect
19 information at rest, in transit, and in use;

20 “(11) assist the development and accelerate the
21 deployment of methods to promote greater software as-
22 surance;

23 “(12) assist the development and accelerate the
24 deployment of tools to securely and automatically up-
25 date software and firmware in use, with limited or no

1 *necessary intervention by users and limited impact*
2 *on concurrently operating systems and processes; and*

3 “(13) *assist in identifying and addressing un-*
4 *identified or future cybersecurity threats.*

5 “(c) *COORDINATION.—In carrying out this section, the*
6 *Under Secretary for Science and Technology shall coordi-*
7 *nate activities with—*

8 “(1) *the Under Secretary appointed pursuant to*
9 *section 103(a)(1)(H);*

10 “(2) *the heads of other relevant Federal depart-*
11 *ments and agencies, as appropriate; and*

12 “(3) *industry and academia.*

13 “(d) *TRANSITION TO PRACTICE.—The Under Secretary*
14 *for Science and Technology shall—*

15 “(1) *support projects carried out under this title*
16 *through the full life cycle of such projects, including*
17 *research, development, testing, evaluation, pilots, and*
18 *transitions;*

19 “(2) *identify mature technologies that address*
20 *existing or imminent cybersecurity gaps in public or*
21 *private information systems and networks of informa-*
22 *tion systems, protect sensitive information within and*
23 *outside networks of information systems, identify and*
24 *support necessary improvements identified during*
25 *pilot programs and testing and evaluation activities,*

1 *and introduce new cybersecurity technologies through-*
2 *out the homeland security enterprise through partner-*
3 *ships and commercialization; and*

4 “(3) *target federally funded cybersecurity re-*
5 *search that demonstrates a high probability of success-*
6 *ful transition to the commercial market within 2*
7 *years and that is expected to have a notable impact*
8 *on the public or private information systems and net-*
9 *works of information systems.*

10 “(e) *DEFINITIONS.—In this section:*

11 “(1) *CYBERSECURITY RISK.—The term ‘cyberse-*
12 *curity risk’ has the meaning given the term in section*
13 *227.*

14 “(2) *HOMELAND SECURITY ENTERPRISE.—The*
15 *term ‘homeland security enterprise’ means relevant*
16 *governmental and nongovernmental entities involved*
17 *in homeland security, including Federal, State, local,*
18 *and tribal government officials, private sector rep-*
19 *resentatives, academics, and other policy experts.*

20 “(3) *INCIDENT.—The term ‘incident’ has the*
21 *meaning given the term in section 227.*

22 “(4) *INFORMATION SYSTEM.—The term ‘informa-*
23 *tion system’ has the meaning given the term in sec-*
24 *tion 3502 of title 44, United States Code.*

1 “(5) *SOFTWARE ASSURANCE.*—*The term ‘soft-*
2 *ware assurance’ means confidence that software—*

3 “(A) *is free from vulnerabilities, either in-*
4 *tentionally designed into the software or acciden-*
5 *tally inserted at any time during the life cycle*
6 *of the software; and*

7 “(B) *functioning in the intended manner.*”.

8 (2) *CLERICAL AMENDMENT.*—*The table of con-*
9 *tents in section 1(b) of the Homeland Security Act of*
10 *2002 (Public Law 107–296; 116 Stat. 2135) is*
11 *amended by inserting after the item relating to the*
12 *second section 319 the following:*

 “*Sec. 321. Cybersecurity research and development.*”.

13 (b) *RESEARCH AND DEVELOPMENT PROJECTS.*—*Sec-*
14 *tion 831 of the Homeland Security Act of 2002 (6 U.S.C.*
15 *391) is amended—*

16 (1) *in subsection (a)—*

17 (A) *in the matter preceding paragraph (1),*
18 *by striking “2017” and inserting “2022”; and*

19 (B) *in paragraph (2), by striking “under*
20 *section 845 of the National Defense Authoriza-*
21 *tion Act for Fiscal Year 1994 (Public Law 103–*
22 *160). In applying the authorities of that section*
23 *845, subsection (c) of that section shall apply*
24 *with respect to prototype projects under this*
25 *paragraph, and the Secretary shall perform the*

1 *functions of the Secretary of Defense under sub-*
2 *section (d) thereof” and inserting “under section*
3 *2371b of title 10, United States Code, and the*
4 *Secretary shall perform the functions of the Sec-*
5 *retary of Defense as prescribed”;*

6 *(2) in subsection (c)—*

7 *(A) in paragraph (1), in the matter pre-*
8 *ceding subparagraph (A), by striking “2017”*
9 *and inserting “2022”; and*

10 *(B) by amending paragraph (2) to read as*
11 *follows:*

12 *“(2) REPORT.—The Secretary shall annually*
13 *submit to the Committee on Homeland Security and*
14 *the Committee on Science, Space, and Technology of*
15 *the House of Representatives and the Committee on*
16 *Homeland Security and Governmental Affairs of the*
17 *Senate a report detailing—*

18 *“(A) the projects for which the authority*
19 *granted by subsection (a) was utilized;*

20 *“(B) the rationale for those utilizations;*

21 *“(C) the funds spent utilizing that author-*
22 *ity;*

23 *“(D) the extent of cost-sharing for those*
24 *projects among Federal and non-Federal sources;*

1 “(E) the extent to which utilization of that
2 authority has addressed a homeland security ca-
3 pability gap or threat to the homeland identified
4 by the Department;

5 “(F) the total amount of payments, if any,
6 that were received by the Federal Government as
7 a result of the utilization of that authority dur-
8 ing the period covered by the report;

9 “(G) the outcome of each project for which
10 that authority was utilized; and

11 “(H) the results of any audits of those
12 projects.”;

13 (3) in subsection (d), by striking “as defined in
14 section 845(e) of the National Defense Authorization
15 Act for Fiscal Year 1994 (Public Law 103–160; 10
16 U.S.C. 2371 note)” and inserting “as defined in sec-
17 tion 2302 of title 10, United States Code”; and

18 (4) by adding at the end the following:

19 “(e) TRAINING.—The Secretary shall develop a train-
20 ing program for acquisitions staff on the utilization of the
21 authority provided under subsection (a) to ensure account-
22 ability and effective management of projects consistent with
23 the Program Management Improvement Accountability Act
24 (Public Law 114–264) and the amendments made by such
25 Act.”.

1 (c) *NO ADDITIONAL FUNDS AUTHORIZED.*—No addi-
2 tional funds are authorized to carry out the requirements
3 of this Act and the amendments made by this Act. Such
4 requirements shall be carried out using amounts otherwise
5 authorized.

Calendar No. 735

115TH CONGRESS
2^D SESSION

S. 278

[Report No. 115-444]

A BILL

To amend the Homeland Security Act of 2002 to provide for innovative research and development, and for other purposes.

DECEMBER 19, 2018

Reported with an amendment