

AMENDMENT NO. _____ Calendar No. _____

Purpose: 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—115th Cong., 2d Sess.

H. R. 2825

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

Referred to the Committee on _____ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT intended to be proposed by Mr. DAINES

Viz:

- 1 At the appropriate place, insert the following:
- 2 **SEC. ____ . CYBERSECURITY RESEARCH AND DEVELOPMENT**
- 3 **PROJECTS.**
- 4 (a) CYBERSECURITY RESEARCH AND DEVELOP-
- 5 MENT.—
- 6 (1) IN GENERAL.—Title III of the Homeland
- 7 Security Act of 2002 (6 U.S.C. 181 et seq.), as
- 8 amended by section 1601(g) of this Act, is amended
- 9 by adding at the end the following:

1 **“SEC. 321. CYBERSECURITY RESEARCH AND DEVELOP-**
2 **MENT.**

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

10 “(b) ACTIVITIES.—The research and development
11 supported under subsection (a) shall serve the components
12 of the Department and shall—

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

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

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

24 “(4) assist the development and support infra-
25 structure and tools to support cybersecurity research
26 and development efforts, including modeling,

1 testbeds, and data sets for assessment of new cyber-
2 security technologies;

3 “(5) assist the development and support of
4 technologies to reduce vulnerabilities in industrial
5 control systems;

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

8 “(7) assist the development and accelerate the
9 deployment of full information life cycle security
10 technologies to enhance protection, control, and pri-
11 vacy of information to detect and prevent cybersecu-
12 rity risks and incidents;

13 “(8) assist the development and accelerate the
14 deployment of information security measures, in ad-
15 dition to perimeter-based protections;

16 “(9) assist the development and accelerate the
17 deployment of technologies to detect improper infor-
18 mation access by authorized users;

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

22 “(11) assist the development and accelerate the
23 deployment of methods to promote greater software
24 assurance;

1 “(12) assist the development and accelerate the
2 deployment of tools to securely and automatically
3 update software and firmware in use, with limited or
4 no necessary intervention by users and limited im-
5 pact on concurrently operating systems and proc-
6 esses; and

7 “(13) assist in identifying and addressing un-
8 identified or future cybersecurity threats.

9 “(c) COORDINATION.—In carrying out this section,
10 the Under Secretary for Science and Technology shall co-
11 ordinate activities with—

12 “(1) the Director of Cybersecurity and Infra-
13 structure Security;

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

16 “(3) industry and academia.

17 “(d) TRANSITION TO PRACTICE.—The Under Sec-
18 retary for Science and Technology shall—

19 “(1) support projects carried out under this
20 title through the full life cycle of such projects, in-
21 cluding research, development, testing, evaluation,
22 pilots, and transitions;

23 “(2) identify mature technologies that address
24 existing or imminent cybersecurity gaps in public or
25 private information systems and networks of infor-

1 mation systems, protect sensitive information within
2 and outside networks of information systems, iden-
3 tify and support necessary improvements identified
4 during pilot programs and testing and evaluation ac-
5 tivities, and introduce new cybersecurity technologies
6 throughout the homeland security enterprise through
7 partnerships and commercialization; and

8 “(3) target federally funded cybersecurity re-
9 search that demonstrates a high probability of suc-
10 cessful transition to the commercial market within 2
11 years and that is expected to have a notable impact
12 on the public or private information systems and
13 networks of information systems.

14 “(e) DEFINITIONS.—In this section:

15 “(1) CYBERSECURITY RISK.—The term ‘cyber-
16 security risk’ has the meaning given the term in sec-
17 tion 2209.

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

24 “(3) INCIDENT.—The term ‘incident’ has the
25 meaning given the term in section 2209.

1 “(4) INFORMATION SYSTEM.—The term ‘infor-
2 mation system’ has the meaning given the term in
3 section 3502 of title 44, United States Code.

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

6 “(A) is free from vulnerabilities, either in-
7 tentionally designed into the software or acci-
8 dentally inserted at any time during the life
9 cycle of the software; and

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

11 (2) CLERICAL AMENDMENT.—The table of con-
12 tents in section 1(b) of the Homeland Security Act
13 of 2002 (Public Law 107–296; 116 Stat. 2135), as
14 amended by this Act, is amended by inserting after
15 the item relating to section 320 the following:

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

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

19 (1) in subsection (a)—

20 (A) in the matter preceding paragraph (1),
21 by striking “2017” and inserting “2022”; and

22 (B) in paragraph (2), by striking “under
23 section 845 of the National Defense Authoriza-
24 tion Act for Fiscal Year 1994 (Public Law
25 103–160). In applying the authorities of that

1 section 845, subsection (c) of that section shall
2 apply with respect to prototype projects under
3 this paragraph, and the Secretary shall perform
4 the functions of the Secretary of Defense under
5 subsection (d) thereof” and inserting “under
6 section 2371b of title 10, United States Code,
7 and the Secretary shall perform the functions of
8 the Secretary of Defense as prescribed.”;

9 (2) in subsection (c)—

10 (A) in paragraph (1), in the matter pre-
11 ceding subparagraph (A), by striking “2017”
12 and inserting “2022”; and

13 (B) by amending paragraph (2) to read as
14 follows:

15 “(2) REPORT.—The Secretary shall annually
16 submit to the Committee on Homeland Security and
17 the Committee on Science, Space, and Technology of
18 the House of Representatives and the Committee on
19 Homeland Security and Governmental Affairs of the
20 Senate a report detailing the projects for which the
21 authority granted by subsection (a) was utilized, the
22 rationale for such utilizations, the funds spent uti-
23 lizing such authority, the extent of cost-sharing for
24 such projects among Federal and non-Federal
25 sources, the extent to which utilization of such au-

1 thority has addressed a homeland security capability
2 gap or threat to the homeland identified by the De-
3 partment, the total amount of payments, if any, that
4 were received by the Federal Government as a result
5 of the utilization of such authority during the period
6 covered by each such report, the outcome of each
7 project for which such authority was utilized, and
8 the results of any audits of such projects.”;

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

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

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

22 (c) NO ADDITIONAL FUNDS AUTHORIZED.—No addi-
23 tional funds are authorized to carry out the requirements
24 of this section and the amendments made by this section.

- 1 Such requirements shall be carried out using amounts oth-
- 2 erwise authorized.