I

115TH CONGRESS
1ST SESSION

H. R. 239

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

IN THE HOUSE OF REPRESENTATIVES

JANUARY 4, 2017

Mr. RATCLIFFE (for himself and Mr. MCCAUL) introduced the following bill; which was referred to the Committee on Homeland Security

---

A BILL

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

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Support for Rapid Innovation Act of 2017''.

SEC. 2. CYBERSECURITY RESEARCH AND DEVELOPMENT PROJECTS.

(a) CYBERSECURITY RESEARCH AND DEVELOPMENT.—

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

"SEC. 321. CYBERSECURITY RESEARCH AND DEVELOPMENT.

''(a) IN GENERAL.—The Under Secretary for Science and Technology shall support the research, development, testing, evaluation, and transition of cybersecurity technologies, including fundamental research to improve the sharing of information, analytics, and methodologies related to cybersecurity risks and incidents, consistent with current law.

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

''(1) advance the development and accelerate the deployment of more secure information systems;

''(2) improve and create technologies for detecting attacks or intrusions, including real-time continuous diagnostics and real-time analytic technologies;

''(3) improve and create mitigation and recovery methodologies, including techniques and policies for real-time containment of attacks, and development of resilient networks and information systems;

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

''(5) develop and support infrastructure and tools to support cybersecurity research and development efforts, including modeling, testbeds, and data sets for assessment of new cybersecurity technologies;

''(6) assist the development and support of technologies to reduce vulnerabilities in industrial control systems; and

''(7) develop and support cyber forensics and attack attribution capabilities.

''(c) COORDINATION.—In carrying out this section, the Under Secretary for Science and Technology shall coordinate activities with—

''(1) the Under Secretary appointed pursuant to section 103(a)(1)(H);

''(2) the heads of other relevant Federal departments and agencies, as appropriate; and

''(3) industry and academia.

''(d) TRANSITION TO PRACTICE.—The Under Secretary for Science and Technology shall support projects carried out under this title through the full life cycle of such projects, including research, development, testing,

evaluation, pilots, and transitions. The Under Secretary shall identify mature technologies that address existing or imminent cybersecurity gaps in public or private information systems and networks of information systems, identify and support necessary improvements identified during pilot programs and testing and evaluation activities, and introduce new cybersecurity technologies throughout the homeland security enterprise through partnerships and commercialization. The Under Secretary shall target federally funded cybersecurity research that demonstrates a high probability of successful transition to the commercial market within two years and that is expected to have a notable impact on the public or private information systems and networks of information systems.

''(e) DEFINITIONS.—In this section:

''(1) CYBERSECURITY RISK.—The term 'cybersecurity risk' has the meaning given such term in section 227.

''(2) HOMELAND SECURITY ENTERPRISE.—The term 'homeland security enterprise' means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and tribal government officials, private sector representatives, academics, and other policy experts.

''(3) INCIDENT.—The term 'incident' has the meaning given such term in section 227.

''(4) INFORMATION SYSTEM.—The term 'information system' has the meaning given such term in section 3502(8) of title 44, United States Code.''.

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to the second section 319 the following new item:

''Sec. 321. Cybersecurity research and development.''.

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

(1) in subsection (a)—

(A) in the matter preceding paragraph (1), by striking ''2016'' and inserting ''2021'';

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

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

''(3) PRIOR APPROVAL.—In any case in which the head of a component or office of the Department seeks to utilize the authority under this section, such head shall first receive prior approval from the Secretary by providing to the Secretary a proposal that includes the rationale for the utilization of such au-

thority, the funds to be spent on the use of such authority, and the expected outcome for each project that is the subject of the use of such authority. In such a case, the authority for evaluating the proposal may not be delegated by the Secretary to anyone other than the Under Secretary for Management.'';

(2) in subsection (c)—

(A) in paragraph (1), in the matter preceding subparagraph (A), by striking ''2016'' and inserting ''2021''; and

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

''(2) REPORT.—The Secretary shall annually submit to the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report detailing the projects for which the authority granted by subsection (a) was utilized, the rationale for such utilizations, the funds spent utilizing such authority, the extent of cost-sharing for such projects among Federal and non-Federal sources, the extent to which utilization of such authority has addressed a homeland security capability

gap or threat to the homeland identified by the Department, the total amount of payments, if any, that were received by the Federal Government as a result of the utilization of such authority during the period covered by each such report, the outcome of each project for which such authority was utilized, and the results of any audits of such projects.''; and

(3) by adding at the end the following new subsection:

''(e) TRAINING.—The Secretary shall develop a training program for acquisitions staff on the utilization of the authority provided under subsection (a).''.

(c) PROHIBITION ON ADDITIONAL FUNDING.—No additional funds are authorized to be appropriated to carry out this Act and the amendments made by this Act.

○