Calendar No. 735

115TH Congress *2d Session*	SENATE	REPORT 115–444

SUPPORT FOR RAPID INNOVATION ACT OF 2017

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 278

TO AMEND THE HOMELAND SECURITY ACT OF 2002 TO PROVIDE FOR INNOVATIVE RESEARCH AND DEVELOPMENT, AND FOR OTHER PURPOSES

DECEMBER 19, 2018.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

89–010 WASHINGTON : 2018

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MICHAEL B. ENZI, Wyoming
JOHN HOEVEN, North Dakota
STEVE DAINES, Montana
JON KYL, Arizona

CLAIRE MCCASKILL, Missouri
THOMAS R. CARPER, Delaware
HEIDI HEITKAMP, North Dakota
GARY C. PETERS, Michigan
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
DOUG JONES, Alabama

CHRISTOPHER R. HIXON, *Staff Director*
GABRIELLE D'ADAMO SINGER, *Chief Counsel*
MICHELLE D. WOODS, *Senior Professional Staff Member*
MARGARET E. DAUM, *Minority Staff Director*
CHARLES A. MOSKOWITZ, *Minority Senior Legislative Counsel*
SUBHASRI RAMANATHAN, *Minority Counsel*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 735

115TH CONGRESS, *2d Session* | SENATE | REPORT 115–444

SUPPORT FOR RAPID INNOVATION ACT OF 2017

DECEMBER 19, 2018.—Ordered to be printed

Mr. JOHNSON, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 278]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 278) to amend the Homeland Security Act of 2002 to provide for innovative research and development, and for other purposes, having considered the same, reports favorably thereon with an amendment in the nature of a substitute and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

The purpose of S. 278, the Support for Rapid Innovation Act of 2018, is to direct the Under Secretary of Science and Technology (S&T) to support the research, development, testing, and evaluation of cybersecurity technologies. It specifies the improvements, creations, and deployments that the research and development activities should produce for the components of the Department of Homeland Security (DHS or the Department). It requires coordination with non-Federal entities, the National Protection and Pro-

89–010

grams Directorate (NPPD), the heads of other relevant Federal departments and agencies, and industry and academia.

II. Background and the Need for Legislation

S. 278 extends the authority of the DHS Under Secretary for S&T to support the research and development of innovative cybersecurity solutions. The Federal Government spends about $80 billion annually on information technology, including activities related to the operation and maintenance of outdated legacy information systems.[1] Less than a quarter of this spending is related to efforts to modernize and develop new information systems.[2] For instance, in May 2016, the Government Accountability Office (GAO) reported that Federal agencies are operating and maintaining information systems that ". . . are inefficient, ineffective, and increasingly obsolete, but federal spending on them has increased over the past 7 fiscal years from about $55 billion to about $63 billion."[3] The Committee is concerned that the Federal Government's efforts to address security vulnerabilities by patching legacy information systems, rather than leveraging available technologies in the private sector, exposes Federal information systems and networks to increased cybersecurity risks.

The effectiveness of the capabilities available to Federal agencies to detect, deter, and remediate malicious cyber intrusions on their information systems has been a longstanding concern of the Committee and oversight entities.[4] In June 2015, the Committee held a hearing entitled, *Under Attack: Federal Cybersecurity and the Office of Personnel Management Data Breach*, which examined cyber threats and vulnerabilities across Federal information systems and networks.[5] Specifically, the hearing examined the Office of Personnel Management's plans to address security vulnerabilities in its systems that resulted in the theft of 4.1 million Federal employee's personnel records, including sensitive background data.[6] During this hearing, Chairman Ron Johnson stated:

> Cybersecurity on federal agency networks has proved to be grossly inadequate. Foreign actors, cyber criminals and hacktivists are accessing our networks with ease and impunity. While our defenses are antiquated, our adversaries are by comparison proving to be highly sophisticated. Meanwhile, agencies are concentrating their resources trying to dictate cybersecurity requirements for private companies, which in many cases are implementing cybersecurity better and more cheaply.[7]

---

[1] Gov't Accountability Office, IT Acquisitions and Operations—High Risk Issue https://www.gao.gov/key_issues/it_acquisitions_operations/issue_summary#t=0 (last visited Nov. 9, 2018).

[2] *Id.*

[3] *Id.*

[4] *Under Attack: Federal Cybersecurity and the OPM Data Breach: Hearing Before the S. Comm. On Homeland Sec. and Gov't Affairs*, 114th Cong. (March 16, 2016), https://www.hsgac.senate.gov/hearings/under-attack-federal-cybersecurity-and-the-opm-data-breach; *Mitigating America's Cybersecurity Risk: Hearing Before the S. Comm. On Homeland Sec. and Gov't Affairs*, 115th Cong. (Apr. 24, 2018), https://www.hsgac.senate.gov/hearings/mitigating-americas-cybersecurity-risk.

[5] *Under Attack: Federal Cybersecurity and the OPM Data Breach: Hearing Before the S. Comm. On Homeland Sec. and Gov't Affairs*, 114th Cong.

[6] *Id.*

[7] *Id.*

In February 2017 testimony before the Subcommittee on Research and Technology, Committee on Science, Space, and Technology of the House of Representatives, Gregory Wilshusen of GAO stated that "(c)yber-based intrusions and attacks on federal systems and systems supporting our nation's critical infrastructure, such as communications and financial services, are evolving and becoming more sophisticated."[8] However, in April 2018, the Committee held a hearing entitled, "*Mitigating America's Cybersecurity Risk*", Mr. Wilshusen stated that DHS has "provided limited intrusion detection and prevention capabilities to entities across the federal government."[9] This statement was based on the findings of a January 2016 GAO report, which found that the DHS's National Cybersecurity Protection System (NCPS), operationally known as EINSTEIN, had limited capabilities for detections and preventing intrusions, conducting analytics, and sharing information.[10] The GAO report further concluded that DHS had not taken actions necessary to ensure the successful mitigation of cybersecurity risks on Federal and private-sector computer systems and networks.[11]

Moreover, the Office of Management and Budget reported in its Annual Federal Information System Modernization Act Report to Congress for Fiscal Year 2017, that from January 2016 through April 2017, DHS's NCPS detected about three percent of cyber incidents across Federal civilian networks via its EINSTEIN sensors.[12]

S. 278 supports DHS's role in improving the security of Federal information systems and networks and addressing cybersecurity gaps in public or private information systems and networks by authorizing the Department to leverage existing cybersecurity technologies in the private sector. Specifically, this bill aims to advance research and development projects that accelerate the deployment of more secure information systems, improves and creates technologies for detecting and preventing attacks or intrusions, and assist the development and support of cyber forensics and attack attribution capabilities.

The bill also extends the Department's authority to conduct a research and development pilot program through September 30, 2022, and includes a provision requiring an annual report to Congress on the projects developed and utilized under this section. Finally, the bill requires the Under Secretary for S&T to develop a training program for acquisitions staff that aims to prevent improper information access by authorized users. No additional funds are authorized to carry out the requirements of this bill.

---

[8] *Strengthening U.S. Cybersecurity Capabilities: Hearing Before H. Comm. on Science, Space, & Tech. Subcomm. On Research and Tech*., 115th Cong. (Feb. 14, 2017) (testimony of Gregory C. Wilshusen, Dir., Info. Sec. Issues, Gov't Accountability Office), https://www.gao.gov/assets/690/682756.pdf.

[9] *Mitigating America's Cybersecurity Risk: Hearing Before the S. Comm. On Homeland Sec. and Gov't Affairs*, 115th Cong. (Apr. 24, 2018).

[10] Gov't Accountability Office, GAO–16–294, Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System (Jan. 28, 2016).

[11] *Id.*

[12] Letter from Suzette Kent, Fed. Chief Info. Officer, Office of e-Government and Info. Tech., Office of Mgmt. & Budget to The Honorable Johnson, Chairman, S. Comm. on Homeland Sec. & Governmental Affairs (Sept. 14, 2018).

III. LEGISLATIVE HISTORY

Senators Steve Daines (R–MT) and Mark R. Warner (D–VA) introduced S. 278 on February 2, 2017. The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 278 at a business meeting on September 26, 2018. Senator Daines offered an amendment in the nature of a substitute that removed the requirement that the DHS Under Secretary for S&T support the review of source code that underpins critical information systems in coordination with non-Federal entities. The Committee adopted the amendment and ordered the bill, as amended, reported favorably, both by voice vote. Senators present for both the vote on the amendment and the vote on the underlying bill were: Johnson, Portman, Lankford, Enzi, Hoeven, McCaskill, Carper, Heitkamp, Peters, Hassan, Harris, and Jones.

IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

Section 1. Short title

This section provides the bill's short title, the "Support for Rapid Innovation Act of 2018".

Section 2. Cybersecurity research and development projects

Subsection (a) amends Title III of the Homeland Security Act of 2002 by adding a new section entitled "Cybersecurity Research and Development".

The new section requires the DHS Under Secretary for S&T to support the research, development, testing, evaluation, and transition of cybersecurity technologies. The supported research should use analytics and methodologies related to cybersecurity risks and incidents to improve the sharing of information and information security.

The section also requires the Department's research and development activities to serve the components of DHS to advance the development and accelerate the deployment of more secure information systems and to assist in identifying and addressing unidentified or future cybersecurity threats. DHS's activities should serve to improve and create technologies for detecting and preventing attacks or intrusions, and create mitigation and recovery methodologies. The Department's research and development is required to assist the development and support of infrastructure and tools to support cybersecurity research and development efforts, technologies to reduce vulnerabilities in industrial control systems, and cyber forensics and attack attribution capabilities. DHS's activities are required to assist the development and accelerate the deployment of full information life cycle security technologies, information security measures, technologies to detect improper information access by authorized users, cryptographic technologies to protect information, methods to promote greater software assurance, and tools to securely and automatically update software and firmware in use.

The new section requires the Under Secretary for S&T to coordinate research and development activities with the Under Secretary for NPPD, the heads of other revenant Federal departments and agencies, and industry and academia.

The section also requires the Under Secretary for S&T to support projects through their full life cycle, identify mature technologies that address existing or imminent cybersecurity gaps in public or private information systems and networks, introduce new cybersecurity technologies, and target Federally-funded cybersecurity research that demonstrates a high probability of successful transition to the commercial market within two years.

The section defines "cybersecurity risk," "homeland security enterprise," "incident," "information system," and "software assurance."

Subsection (b) amends Section 831 of the Homeland Security Act of 2002 to extend the Secretary of DHS's authority to conduct research and development programs until September 30, 2022. It also amends Section 831(a)(2) of the Homeland Security Act of 2002, clarifying that the Secretary of DHS may carryout prototype projects in accordance with the requirements Congress established for the Secretary of Defense under section 2371b of title 10, United States Code. The subsection also updated the report language by removing and adding certain congressional committees and requiring that the report include the extent of cost-sharing for projects among Federal and non-Federal sources, the extent to which utilization of the authority has addressed a homeland security capability gap or threat, the amount of payments that were received by the Federal Government as a result of the utilization of the authority, and the outcome of each project. It also requires the Secretary to develop a training program for acquisitions staff on the proper use of the research and development authorities to ensure accountability and effective management of the projects.

Section (c) provides that no additional funds are authorized. If additional funds are required to carry out the requirements, the funds must be used from other funding authorizations.

V. Evaluation of Regulatory Impact

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. Congressional Budget Office Cost Estimate

CBO failed to provide the Committee with a cost estimate in time for the final reporting deadline of the 115th Congress.

VII. Changes in Existing Law Made by the Bill, as Reported

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows: (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

* * * * * * *

SEC. 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Homeland Security Act of 2002."

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

* * * * * * *

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, information security, 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 and preventing attacks or intrusions, including real-time continuous diagnostics, real-time analytic technologies, and full life cycle information protection;

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

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

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

(7) assist the development and accelerate the deployment of full information life cycle security technologies to enhance protection, control, and privacy of information to detect and prevent cybersecurity risks and incidents;

(8) assist the development and accelerate the deployment of information security measures, in addition to perimeter-based protections;

(9) assist the development and accelerate the deployment of technologies to detect improper information access by authorized users;

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

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

(12) assist the development and accelerate the deployment of tools to securely and automatically update software and firmware in use, with limited or no necessary intervention by users and limited impact on concurrently operating systems and processes; and

(13) assist in identifying and addressing unidentified or future cybersecurity threats.

(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—

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

(2) identify mature technologies that address existing or imminent cybersecurity gaps in public or private information systems and networks of information systems, protect sensitive information within and outside 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; and

(3) target federally funded cybersecurity research that demonstrates a high probability of successful transition to the commercial market within 2 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 the 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 the term in section 227.

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

(5) SOFTWARE ASSURANCE.—The term 'software assurance' means confidence that software—

(A) is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during the life cycle of the software; and

(B) functioning in the intended manner.

* * * * * * *

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

* * * * * * *

Subtitle D—Acquisitions

* * * * * * *

SEC. 831. RESEARCH AND DEVELOPMENT PROJECTS.

(a) AUTHORITY.—Until September 30, [2017] *2022,* and subject to subsection (d), the Secretary may carry out a pilot program under which the Secretary may exercise the following authorities:

(1) * * *

(2) PROTOTYPE PROJECTS.—The Secretary may, under the authority of paragraph (1), carry out prototype projects in accordance with the requirements and conditions provided for carrying out prototype projects [under section 845 of the National Defense Authorization Act for Fiscal Year 1994 (Public Law 103–160). In applying the authorities of that section 845, subsection (c) of that section shall apply with respect to prototype projects under this paragraph, and the Secretary shall perform the functions of the Secretary of Defense under subsection (d) thereof] *under section 2371b of title 10, United States Code, and the Secretary shall perform the functions of the Secretary of Defense as prescribed.*

(b) * * *

(c) ADDITIONAL REQUIREMENTS.—

(1) IN GENERAL.—The authority of the Secretary under this section shall terminate September 30, [2017] *2022,* unless before that date the Secretary—

(A) * * *

(B) * * *

[(2) REPORT.—The Secretary shall provide an annual report to the Committees on Appropriations of the Senate and the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives detailing the projects for which the authority granted by subsection (a) was used, the rationale for its use, the funds spent using that authority, the outcome of each project for which

that authority was used, and the results of any audits of such projects.]

(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—

(A) the projects for which the authority granted by subsection (a) was utilized;

(B) the rationale for those utilizations;

(C) the funds spent utilizing that authority;

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

(E) the extent to which utilization of that authority has addressed a homeland security capability gap or threat to the homeland identified by the Department;

(F) the total amount of payments, if any, that were received by the Federal Government as a result of the utilization of that authority during the period covered by each such report;

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

(H) the results of any audits of those projects.

(d) DEFINITION OF NONTRADITIONAL GOVERNMENT CONTRACTOR.—In this section, the term "nontraditional Government contractor" has the same meaning as the term "nontraditional defense contractor" [as defined in section 845(e) of the National Defense Authorization Act for Fiscal Year 1994 (Public Law 103 160; 10 U.S.C. 2371 note)] *as defined in section 2302 of title 10, United States Code*.

(e) TRAINING.—The Secretary shall develop a training program for acquisitions staff on the utilization of the authority provided under subsection (a) to ensure accountability and effective management of projects consistent with the Program Management Improvement Accountability Act (Public Law 114 264) and the amendments made by such Act.

○