115TH CONGRESS
2D SESSION

S. 3464

To amend the Homeland Security Act of 2002 to authorize the Secretary of Homeland Security to establish a continuous diagnostics and mitigation program at the Department of Homeland Security, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 18, 2018

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

---

A BILL

To amend the Homeland Security Act of 2002 to authorize the Secretary of Homeland Security to establish a continuous diagnostics and mitigation program at the Department of Homeland Security, 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 ''Advancing Cybersecurity Diagnostics and Mitigation Act''.

SEC. 2. ESTABLISHMENT OF CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM IN DEPARTMENT OF HOMELAND SECURITY.

(a) IN GENERAL.—Section 230 of the Homeland Security Act of 2002 (6 U.S.C. 151) is amended by adding at the end the following new subsection:

''(g) CONTINUOUS DIAGNOSTICS AND MITIGATION.—

''(1) PROGRAM.—

''(A) IN GENERAL.—The Secretary shall deploy, operate, and maintain a continuous diagnostics and mitigation program. Under such program, the Secretary shall—

''(i) develop and provide the capability to collect, analyze, and visualize information relating to security data and cybersecurity risks;

''(ii) make program capabilities available for use, with or without reimbursement;

''(iii) employ shared services, collective purchasing, blanket purchase agreements, and any other economic or procurement models the Secretary determines appropriate to maximize the costs savings associated with implementing an information system;

''(iv) assist entities in setting information security priorities and managing cybersecurity risks; and

''(v) develop policies and procedures for reporting systemic cybersecurity risks and potential incidents based upon data collected under such program.

''(B) REGULAR IMPROVEMENT.—The Secretary shall regularly deploy new technologies and modify existing technologies to the continuous diagnostics and mitigation program required under subparagraph (A), as appropriate, to improve the program.

''(2) ACTIVITIES.—In carrying out the continuous diagnostics and mitigation program under paragraph (1), the Secretary shall ensure, to the extent practicable, that—

''(A) timely, actionable, and relevant cybersecurity risk information, assessments, and analysis are provided in real time;

''(B) share the analysis and products developed under such program;

''(C) all information, assessments, analyses, and raw data under such program is made available to the national cybersecurity and com-

munications integration center of the Department; and

"(D) provide regular reports on cybersecurity risks.".

(b) CONTINUOUS DIAGNOSTICS AND MITIGATION STRATEGY.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall develop a comprehensive continuous diagnostics and mitigation strategy to carry out the continuous diagnostics and mitigation program required under subsection (g) of section 230 of the Homeland Security Act of 2002 (6 U.S.C. 151), as added by subsection (a).

(2) SCOPE.—The strategy required under paragraph (1) shall include the following:

(A) A description of the continuous diagnostics and mitigation program, including efforts by the Secretary of Homeland Security to assist with the deployment of program tools, capabilities, and services, from the inception of the program referred to in paragraph (1) to the date of the enactment of this Act.

(B) A description of the coordination required to deploy, install, and maintain the tools,

capabilities, and services that the Secretary of Homeland Security determines to be necessary to satisfy the requirements of such program.

(C) A description of any obstacles facing the deployment, installation, and maintenance of tools, capabilities, and services under such program.

(D) Recommendations and guidelines to help maintain and continuously upgrade tools, capabilities, and services provided under such program.

(E) Recommendations for using the data collected by such program for creating a common framework for data analytics, visualization of enterprise-wide risks, and real-time reporting.

(F) Recommendations for future efforts and activities, including for the rollout of new tools, capabilities and services, proposed timelines for delivery, and whether to continue the use of phased rollout plans, related to securing networks, devices, data, and information technology assets through the use of such program.

(3) FORM.—The strategy required under subparagraph (A) shall be submitted in an unclassified form, but may contain a classified annex.

(c) REPORT.—Not later than 90 days after the development of the strategy required under subsection (b), the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representative a report on cybersecurity risk posture based on the data collected through the continuous diagnostics and mitigation program under subsection (g) of section 230 of the Homeland Security Act of 2002 (6 U.S.C. 151), as added by subsection (a).

○