

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.

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 “Advancing Cybersecu-
5 rity Diagnostics and Mitigation Act”.

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

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

7 “(g) CONTINUOUS DIAGNOSTICS AND MITIGATION.—
8 “(1) PROGRAM.—

9 “(A) IN GENERAL.—The Secretary shall
10 deploy, operate, and maintain a continuous
11 diagnostics and mitigation program. Under
12 such program, the Secretary shall—

13 “(i) develop and provide the capability
14 to collect, analyze, and visualize informa-
15 tion relating to security data and cyberse-
16 curity risks;

17 “(ii) make program capabilities avail-
18 able for use, with or without reimburse-
19 ment;

20 “(iii) employ shared services, collective
21 purchasing, blanket purchase agreements,
22 and any other economic or procurement
23 models the Secretary determines appro-
24 priate to maximize the costs savings asso-
25 ciated with implementing an information
26 system;

1 “(iv) assist entities in setting informa-
2 tion security priorities and managing cy-
3 bersecurity risks; and

4 “(v) develop policies and procedures
5 for reporting systemic cybersecurity risks
6 and potential incidents based upon data
7 collected under such program.

8 “(B) REGULAR IMPROVEMENT.—The Sec-
9 retary shall regularly deploy new technologies
10 and modify existing technologies to the contin-
11 uous diagnostics and mitigation program re-
12 quired under subparagraph (A), as appropriate,
13 to improve the program.

14 “(2) ACTIVITIES.—In carrying out the contin-
15 uous diagnostics and mitigation program under
16 paragraph (1), the Secretary shall ensure, to the ex-
17 tent practicable, that—

18 “(A) timely, actionable, and relevant cyber-
19 security risk information, assessments, and
20 analysis are provided in real time;

21 “(B) share the analysis and products de-
22 veloped under such program;

23 “(C) all information, assessments, anal-
24 yses, and raw data under such program is made
25 available to the national cybersecurity and com-

1 communications integration center of the Depart-
2 ment; and

3 “(D) provide regular reports on cybersecu-
4 rity risks.”.

5 (b) CONTINUOUS DIAGNOSTICS AND MITIGATION
6 STRATEGY.—

7 (1) IN GENERAL.—Not later than 180 days
8 after the date of the enactment of this Act, the Sec-
9 retary of Homeland Security shall develop a com-
10 prehensive continuous diagnostics and mitigation
11 strategy to carry out the continuous diagnostics and
12 mitigation program required under subsection (g) of
13 section 230 of the Homeland Security Act of 2002
14 (6 U.S.C. 151), as added by subsection (a).

15 (2) SCOPE.—The strategy required under para-
16 graph (1) shall include the following:

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

24 (B) A description of the coordination re-
25 quired to deploy, install, and maintain the tools,

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

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

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

12 (E) Recommendations for using the data
13 collected by such program for creating a com-
14 mon framework for data analytics, visualization
15 of enterprise-wide risks, and real-time report-
16 ing.

17 (F) Recommendations for future efforts
18 and activities, including for the rollout of new
19 tools, capabilities and services, proposed
20 timelines for delivery, and whether to continue
21 the use of phased rollout plans, related to se-
22 curing networks, devices, data, and information
23 technology assets through the use of such pro-
24 gram.

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

4 (c) REPORT.—Not later than 90 days after the devel-
5 opment of the strategy required under subsection (b), the
6 Secretary of Homeland Security shall submit to the Com-
7 mittee on Homeland Security and Governmental Affairs
8 of the Senate and the Committee on Homeland Security
9 of the House of Representative a report on cybersecurity
10 risk posture based on the data collected through the con-
11 tinuous diagnostics and mitigation program under sub-
12 section (g) of section 230 of the Homeland Security Act
13 of 2002 (6 U.S.C. 151), as added by subsection (a).

○