

115TH CONGRESS
2D SESSION

H. R. 6443

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 5, 2018

Received; read twice and referred to the Committee on Homeland Security and
Governmental Affairs

AN ACT

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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Advancing Cybersecu-
3 rity Diagnostics and Mitigation Act”.

4 **SEC. 2. ESTABLISHMENT OF CONTINUOUS DIAGNOSTICS**
5 **AND MITIGATION PROGRAM IN DEPARTMENT**
6 **OF HOMELAND SECURITY.**

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

10 “(g) CONTINUOUS DIAGNOSTICS AND MITIGATION.—

11 “(1) PROGRAM.—

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

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

20 “(ii) make program capabilities avail-
21 able for use, with or without reimburse-
22 ment;

23 “(iii) employ shared services, collective
24 purchasing, blanket purchase agreements,
25 and any other economic or procurement
26 models the Secretary determines appro-

1 priate to maximize the costs savings asso-
2 ciated with implementing an information
3 system;

4 “(iv) assist entities in setting informa-
5 tion security priorities and managing cy-
6 bersecurity risks; and

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

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

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

21 “(A) timely, actionable, and relevant cyber-
22 security risk information, assessments, and
23 analysis are provided in real time;

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

“(C) all information, assessments, analyses, and raw data under such program is made available to the national cybersecurity and communications 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 such Act, 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.

1 (B) A description of the coordination re-
2 quired to deploy, install, and maintain the tools,
3 capabilities, and services that the Secretary of
4 Homeland Security determines to be necessary
5 to satisfy the requirements of such program.

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

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

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

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

1 technology assets through the use of such pro-
2 gram.

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

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

 Passed the House of Representatives September 4,
2018.

Attest:

KAREN L. HAAS,

Clerk.