

116TH CONGRESS
1ST SESSION

H. R. 4237

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

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 6, 2019

Mr. RATCLIFFE (for himself and Mr. KHANNA) introduced the following bill; which was referred to the Committee on Oversight and Reform, and in addition to the Committee on Homeland Security, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

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 in the Cybersecurity and Infrastructure Security Agency of 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 THE CYBER-**
3 **SECURITY AND INFRASTRUCTURE SECURITY**
4 **AGENCY.**

5 (a) IN GENERAL.—Section 2213 of the Homeland
6 Security Act of 2002 (6 U.S.C. 663) is amended by adding
7 at the end the following:

8 “(g) CONTINUOUS DIAGNOSTICS AND MITIGATION.—

9 “(1) PROGRAM.—

10 “(A) IN GENERAL.—The Secretary, acting
11 through the Director of Cybersecurity and In-
12 frastructure Security, shall deploy, operate, and
13 maintain a continuous diagnostics and mitiga-
14 tion program for agencies. Under such pro-
15 gram, the Secretary shall—

16 “(i) assist agencies to continuously di-
17 agnose and mitigate cyber threats and
18 vulnerabilities;

19 “(ii) develop and provide the capa-
20 bility to collect, analyze, and visualize in-
21 formation relating to security data and cy-
22 bersecurity risks at agencies;

23 “(iii) make program capabilities avail-
24 able for use, with or without reimburse-
25 ment, to civilian agencies and State, local,
26 Tribal, and territorial governments;

1 “(iv) employ shared services, collective
2 purchasing, blanket purchase agreements,
3 and any other economic or procurement
4 models the Secretary determines appro-
5 priate to maximize the costs savings asso-
6 ciated with implementing an information
7 system;

8 “(v) assist entities in setting informa-
9 tion security priorities and assessing and
10 managing cybersecurity risks; and

11 “(vi) develop policies and procedures
12 for reporting systemic cybersecurity risks
13 and potential incidents based upon data
14 collected under such program.

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

21 “(2) AGENCY RESPONSIBILITIES.—Notwith-
22 standing any other provision of law, each agency
23 that uses the continuous diagnostics and mitigation
24 program under paragraph (1) shall, continuously
25 and in real time, provide to the Secretary all infor-

1 mation, assessments, analyses, and raw data col-
2 lected by the program, in a manner specified by the
3 Secretary.

4 “(3) RESPONSIBILITIES OF THE SECRETARY.—
5 In carrying out the continuous diagnostics and miti-
6 gation program under paragraph (1), the Secretary
7 shall, as appropriate—

8 “(A) share with agencies relevant analysis
9 and products developed under such program;

10 “(B) provide regular reports on cybersecu-
11 rity risks to agencies; and

12 “(C) provide comparative assessments of
13 cybersecurity risks for agencies.”.

14 (b) CONTINUOUS DIAGNOSTICS AND MITIGATION
15 STRATEGY.—

16 (1) IN GENERAL.—Not later than 180 days
17 after the date of the enactment of this Act, the Sec-
18 retary of Homeland Security shall develop a com-
19 prehensive continuous diagnostics and mitigation
20 strategy to carry out the continuous diagnostics and
21 mitigation program required under subsection (g) of
22 section 2213 of the Homeland Security Act of 2002
23 (6 U.S.C. 663), as added by subsection (a).

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

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

8 (B) A description of the coordination and
9 funding required to deploy, install, and main-
10 tain the tools, capabilities, and services that the
11 Secretary of Homeland Security determines to
12 be necessary to satisfy the requirements of such
13 program.

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

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

22 (E) Recommendations for using the data
23 collected by such program for creating a com-
24 mon framework for data analytics, visualization
25 of enterprise-wide risks, and real-time report-

1 ing, and comparative assessments for cyberse-
2 curity risks.

3 (F) Recommendations for future efforts
4 and activities, including for the rollout of new
5 and emerging tools, capabilities and services,
6 proposed timelines for delivery, and whether to
7 continue the use of phased rollout plans, related
8 to securing networks, devices, data, and infor-
9 mation and operational technology assets
10 through the use of such program.

11 (3) FORM.—The strategy required under para-
12 graph (1) shall be submitted in an unclassified form,
13 but may contain a classified annex.

14 (c) REPORT.—Not later than 180 days after the de-
15 velopment of the strategy required under subsection (b),
16 the Secretary of Homeland Security shall submit to the
17 Committee on Homeland Security and Governmental Af-
18 fairs of the Senate and the Committee on Homeland Secu-
19 rity of the House of Representative a report on cybersecu-
20 rity risk posture based on the data collected through the
21 continuous diagnostics and mitigation program under sub-
22 section (g) of section 2213 of the Homeland Security Act
23 of 2002 (6 U.S.C. 663), as added by subsection (a).

24 (d) GAO REPORT.—Not later than 1 year after the
25 date of enactment of this Act, the Comptroller General

1 of the United States shall submit a report to Congress
2 on the potential impacts and benefits of replacing the re-
3 porting requirements under chapter 35 of title 44, United
4 States Code, with periodical real-time data provided by the
5 continuous diagnostics and mitigation program under sub-
6 section (g) of section 2213 of the Homeland Security Act
7 of 2002 (6 U.S.C. 663), as added by subsection (a).

○