

.....  
(Original Signature of Member)

115TH CONGRESS  
2D SESSION

**H. R.** \_\_\_\_\_

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 HOUSE OF REPRESENTATIVES

Mr. RATCLIFFE introduced the following bill; which was referred to the Committee on \_\_\_\_\_

---

**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 Govern-  
15 ment-wide information relating to security  
16 data and cybersecurity risks;

17 “(ii) make program capabilities avail-  
18 able for use by any Federal agency, with or  
19 without reimbursement;

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 agency infor-  
26 mation system;

1                   “(iv) assist officials in setting infor-  
2                   mation security priorities and managing  
3                   cybersecurity 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 to any Fed-  
21                         eral agency;

22                         “(B) share the analysis and products de-  
23                         veloped under such program with Federal and  
24                         non-Federal entities;

1           “(C) all information, assessments, anal-  
2           yses, and raw data under such program is made  
3           available to the national cybersecurity and com-  
4           munications integration center of the Depart-  
5           ment; and

6           “(D) provide regular reports on cybersecu-  
7           rity risks to Federal agencies.”.

8           (b) CONTINUOUS DIAGNOSTICS AND MITIGATION  
9 STRATEGY.—

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

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

19           (A) A description of the continuous  
20           diagnostics and mitigation program, including  
21           efforts by the Secretary of Homeland Security  
22           to assist with the deployment of program tools,  
23           capabilities, and services at Federal agencies,  
24           from the inception of the program referred to

1 in paragraph (1) to the date of the enactment  
2 of this Act.

3 (B) A description of the coordination re-  
4 quired by Federal agencies to deploy, install,  
5 and maintain the tools, capabilities, and serv-  
6 ices that the Secretary of Homeland Security  
7 determines to be necessary to satisfy the re-  
8 quirements of such program.

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

13 (D) Recommendations and guidelines for  
14 Federal agencies to help maintain and continu-  
15 ously upgrade tools, capabilities, and services  
16 provided under such program.

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

22 (F) Recommendations for future efforts  
23 and activities related to securing Federal net-  
24 works, devices, data, and information tech-  
25 nology assets through the use of such program.

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 the cybersecu-  
10          rity risk posture of the Federal enterprise based on the  
11          data collected through the continuous diagnostics and  
12          mitigation program under subsection (g) of section 230  
13          of the Homeland Security Act of 2002, as added by sub-  
14          section (a).