

117TH CONGRESS
2D SESSION

S. 3894

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 SENATE OF THE UNITED STATES

MARCH 22, 2022

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 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 Through Continuous Diagnostics and Mitigation
6 Act”.

1 **SEC. 2. ESTABLISHMENT OF FEDERAL INTRUSION DETEC-**
2 **TION AND PREVENTION SYSTEM AND CON-**
3 **TINUOUS DIAGNOSTICS AND MITIGATION**
4 **PROGRAM IN THE CYBERSECURITY AND IN-**
5 **FRASTRUCTURE SECURITY AGENCY.**

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

9 “(g) CONTINUOUS DIAGNOSTICS AND MITIGATION.—

10 “(1) PROGRAM.—

11 “(A) IN GENERAL.—The Secretary, acting
12 through the Director, shall, with or without re-
13 imbursement, deploy, operate, and maintain a
14 continuous diagnostics and mitigation program
15 for agencies under which 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) employ shared services, collective
24 purchasing, blanket purchase agreements,
25 and any other economic or procurement
26 models the Secretary determines appro-

1 appropriate to maximize the costs savings asso-
2 ciated with implementing the program;

3 “(iv) assist agencies in setting infor-
4 mation security priorities and assessing
5 and managing cybersecurity risks;

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

10 “(vi) promote the adoption of a zero
11 trust security model in improving agency
12 cybersecurity readiness.

13 “(B) REGULAR IMPROVEMENT.—The Sec-
14 retary shall regularly—

15 “(i) deploy new technologies and mod-
16 ify existing technologies to the continuous
17 diagnostics and mitigation program re-
18 quired under subparagraph (A), as appro-
19 priate, to improve the program; and

20 “(ii) update the technical require-
21 ments documentation of the continuous
22 diagnostics and mitigation program re-
23 quired under subparagraph (A) to account
24 for emerging technology capabilities such

1 as cloud computing and comprehensive
2 cloud security controls.

3 “(2) AGENCY RESPONSIBILITIES.—Notwith-
4 standing any other provision of law, each agency
5 that uses the continuous diagnostics and mitigation
6 program under paragraph (1) shall, continuously
7 and in real time, provide to and allow access for the
8 Secretary to collect all information, assessments,
9 analyses, and raw data collected by the program, in
10 a manner specified by the Secretary.

11 “(3) RESPONSIBILITIES OF THE SECRETARY.—
12 In carrying out the continuous diagnostics and miti-
13 gation program under paragraph (1), the Secretary,
14 acting through the Director, shall—

15 “(A) share with agencies relevant analysis
16 and products developed under the program;

17 “(B) provide regular reports on cybersecu-
18 rity risks to agencies;

19 “(C) provide comparative assessments of
20 cybersecurity risks for agencies;

21 “(D) oversee the integration of continuous
22 diagnostics and mitigation products and serv-
23 ices into agency systems;

24 “(E) establish performance requirements
25 for product integrators;

“(F) at the request of an agency, provide technical assistance in selecting, procuring, and integrating continuous diagnostics and mitigation products and services;

“(G) not less than once each fiscal year, submit to the appropriate committees of Congress a report that includes—

“(i) the progress made by each agency to meet continuous diagnostics and mitigation benchmarks from the beginning of the implementation through the date of the report; and

“(ii) a summary of the efforts of each agency to account for emerging technology capabilities; and

“(H) take steps to ensure that the security data collected through the program is aggregated with other Government-wide cybersecurity programs to better automate defensive capabilities.”.

(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 com-

1 prehensive continuous diagnostics and mitigation
2 strategy to carry out the continuous diagnostics and
3 mitigation program required under subsection (g) of
4 section 2213 of the Homeland Security Act of 2002
5 (6 U.S.C. 663), as added by subsection (a).

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

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

18 (C) Guidelines to help maintain and con-
19 tinuously upgrade tools, capabilities, and serv-
20 ices provided under such program.

21 (D) A plan for using the data collected by
22 such program for creating a common frame-
23 work for data analytics, visualization of enter-
24 prise-wide risks, and real-time reporting, and
25 comparative assessments for cybersecurity risks.

(E) Recommendations for using the data to enable the Cybersecurity and Infrastructure Security Agency to engage in cyber hunt and detection and response activities.

(F) Recommendations for future efforts and activities, including for the rollout of new and emerging 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 and operational technology assets through the use of such program.

(G) Recommendations for improving the integration process of continuous diagnostics and mitigation products and capabilities within agency systems.

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

SEC. 3. FEDERAL INTRUSION DETECTION AND PREVENTION SYSTEM AND CONTINUOUS DIAGNOSTICS AND MITIGATION PILOT PROGRAM FOR STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS.

(a) DEFINITIONS.—In this section—

1 (1) the terms “local government” and “State”
2 have the meanings given those terms in section 3 of
3 the Homeland Security Act of 2002 (6 U.S.C. 101);

4 (2) the term “Secretary” means the Secretary
5 of Homeland Security; and

6 (3) the term “Tribal government” means the
7 recognized governing body of any Indian or Alaska
8 Native Tribe, band, nation, pueblo, village, commu-
9 nity, component band, or component reservation,
10 that is individually identified (including parentheti-
11 cally) in the most recent list published pursuant to
12 section 104 of the Federally Recognized Indian
13 Tribe List Act of 1994 (25 U.S.C. 5131).

14 (b) ESTABLISHMENT.—The Secretary shall conduct
15 a Continuous Diagnostics and Mitigation Pilot Program
16 with not less than 5 State, local, Tribal, or territorial gov-
17 ernments to—

18 (1) promote the use of technologies and services
19 in the continuous diagnostics and mitigation pro-
20 gram described in subsection (g) of section 2213 of
21 the Homeland Security Act of 2002 (6 U.S.C. 663),
22 as added by section 2 of this Act, at the State, local,
23 Tribal, and territorial government level;

24 (2) with or without reimbursement, make ac-
25 cessing the technologies and services described in

1 paragraph (1) by State, local, Tribal, and territorial
2 governments as affordable and simple as possible;

3 (3) promote the adoption of a zero trust secu-
4 rity model in improving cybersecurity readiness at
5 the State, local, Tribal, and territorial government
6 level; and

7 (4) provide technical assistance in integrating
8 continuous diagnostics and mitigation technologies
9 and products into State, local, Tribal, and territorial
10 government systems.

11 (c) CONSIDERATIONS.—In selecting a State, local, or
12 Tribal government for participation in the pilot program
13 established under subsection (b), the Secretary shall con-
14 sider—

15 (1) the extent to which the State, local, Tribal,
16 or territorial government aligns its cybersecurity
17 policies with the Center for Internet Security Crit-
18 ical Security Controls, the National Institute of
19 Standards and Technology Cybersecurity Frame-
20 work, or other widely accepted cybersecurity frame-
21 works; and

22 (2) the capability of the State, local, Tribal, or
23 territorial government to deploy and maintain over
24 time continuous diagnostics and mitigation products
25 and services.

1 (d) PROGRAM REQUIREMENTS.—The pilot program
2 established under this section—

3 (1) may not require participants to utilize cer-
4 tain strategies or tools, and shall allow participants
5 to select and integrate tools for meeting the objec-
6 tives of the pilot program; and

7 (2) shall include comprehensive training cur-
8 riculum and integration assistance to close the tech-
9 nical expertise gap between employees of State,
10 local, Tribal, and territorial governments and em-
11 ployees of the Cybersecurity and Infrastructure Se-
12 curity Agency.

13 (e) REPORT.—Not later than 180 days after the date
14 on which the pilot program terminates under this section,
15 the Secretary shall submit to Congress a report that in-
16 cludes—

17 (1) an assessment of the replicability and the
18 costs and benefits of conducting a permanent State,
19 local, Tribal, and territorial government continuous
20 diagnostics and mitigation program as described in
21 subsection (g) of section 2213 of the Homeland Se-
22 curity Act of 2002 (6 U.S.C. 663), as added by sec-
23 tion 2 of this Act;

24 (2) the extent to which State, local, Tribal, and
25 territorial governments in the pilot program adhere

1 to widely accepted cybersecurity standards and
2 frameworks and the impact that those policies have
3 on potential widespread sub-Federal continuous
4 diagnostics and mitigation integration; and

5 (3) an assessment of the cybersecurity readi-
6 ness of participants in the pilot program established
7 under this section prior to participation in the pilot
8 program as compared to after completion of the pilot
9 program.

10 (f) TERMINATION.—The authority to conduct the
11 pilot program under subsections (a) through (d) shall ter-
12minate on the date that is 3 years after the date of enact-
13ment of this Act.

○