117TH CONGRESS
2D SESSION

S. _____

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

and Ms. Hassan _____

Mr. CORNYN introduced the following bill; which was read twice and 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 in the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Advancing Cybersecurity Through Continuous Diagnostics and Mitigation Act".

SEC. 2. ESTABLISHMENT OF FEDERAL INTRUSION DETECTION AND PREVENTION SYSTEM AND CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM IN THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

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

"(g) CONTINUOUS DIAGNOSTICS AND MITIGATION.—

"(1) PROGRAM.—

"(A) IN GENERAL.—The Secretary, acting through the Director, shall, with or without reimbursement, deploy, operate, and maintain a continuous diagnostics and mitigation program for agencies under which the Secretary shall—

"(i) assist agencies to continuously diagnose and mitigate cyber threats and vulnerabilities;

"(ii) develop and provide the capability to collect, analyze, and visualize information relating to security data and cybersecurity risks at agencies;

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

priate to maximize the costs savings associated with implementing the program;

"(iv) assist agencies in setting information security priorities and assessing and managing cybersecurity risks;

"(v) develop policies and procedures for reporting systemic cybersecurity risks and potential incidents based upon data collected under the program; and

"(vi) promote the adoption of a zero trust security model in improving agency cybersecurity readiness.

"(B) REGULAR IMPROVEMENT.—The Secretary shall regularly—

"(i) deploy new technologies and modify existing technologies to the continuous diagnostics and mitigation program required under subparagraph (A), as appropriate, to improve the program; and

"(ii) update the technical requirements documentation of the continuous diagnostics and mitigation program required under subparagraph (A) to account for emerging technology capabilities such

as cloud computing and comprehensive cloud security controls.

"(2) AGENCY RESPONSIBILITIES.—Notwithstanding any other provision of law, each agency that uses the continuous diagnostics and mitigation program under paragraph (1) shall, continuously and in real time, provide to and allow access for the Secretary to collect all information, assessments, analyses, and raw data collected by the program, in a manner specified by the Secretary.

"(3) RESPONSIBILITIES OF THE SECRETARY.—In carrying out the continuous diagnostics and mitigation program under paragraph (1), the Secretary, acting through the Director, shall—

"(A) share with agencies relevant analysis and products developed under the program;

"(B) provide regular reports on cybersecurity risks to agencies;

"(C) provide comparative assessments of cybersecurity risks for agencies;

"(D) oversee the integration of continuous diagnostics and mitigation products and services into agency systems;

"(E) establish performance requirements 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-

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

(2) SCOPE.—The strategy required under paragraph (1) shall include the following:

(A) A description of the coordination and funding required to deploy, install, and maintain the tools, capabilities, and services that the Secretary of Homeland Security determines to be necessary to satisfy the requirements of such program.

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

(C) Guidelines to help maintain and continuously upgrade tools, capabilities, and services provided under such program.

(D) A plan for using the data collected by such program for creating a common framework for data analytics, visualization of enterprise-wide risks, and real-time reporting, and 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) the terms "local government" and "State" have the meanings given those terms in section 3 of the Homeland Security Act of 2002 (6 U.S.C. 101);

(2) the term "Secretary" means the Secretary of Homeland Security; and

(3) the term "Tribal government" means the recognized governing body of any Indian or Alaska Native Tribe, band, nation, pueblo, village, community, component band, or component reservation, that is individually identified (including parenthetically) in the most recent list published pursuant to section 104 of the Federally Recognized Indian Tribe List Act of 1994 (25 U.S.C. 5131).

(b) ESTABLISHMENT.—The Secretary shall conduct a Continuous Diagnostics and Mitigation Pilot Program with not less than 5 State, local, Tribal, or territorial governments to—

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

(2) with or without reimbursement, make accessing the technologies and services described in

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

(3) promote the adoption of a zero trust security model in improving cybersecurity readiness at the State, local, Tribal, and territorial government level; and

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

(c) CONSIDERATIONS.—In selecting a State, local, or Tribal government for participation in the pilot program established under subsection (b), the Secretary shall consider—

(1) the extent to which the State, local, Tribal ,or territorial government aligns its cybersecurity policies with the Center for Internet Security Critical Security Controls, the National Institute of Standards and Technology Cybersecurity Framework, or other widely-accepted cybersecurity frameworks; and

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

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

(1) may not require participants to utilize certain strategies or tools, and shall allow participants to select and integrate tools for meeting the objectives of the pilot program; and

(2) shall include comprehensive training curriculum and integration assistance to close the technical expertise gap between employees of State, local, Tribal, and territorial governments and employees of the Cybersecurity and Infrastructure Security Agency.

(e) REPORT.—Not later than 180 days after the date on which the pilot program terminates under this section, the Secretary shall submit to Congress a report that includes—

(1) an assessment of the replicability and the costs and benefits of conducting a permanent State, local, Tribal, and territorial government continuous diagnostics and mitigation program as described in subsection (g) of section 2213 of the Homeland Security Act of 2002 (6 U.S.C. 663), as added by section 2 of this Act;

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

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

(3) an assessment of the cybersecurity readiness of participants in the pilotv program established under this section prior to participation in the pilot program as compared to after completion of the pilot program.

(f) TERMINATION.—The authority to conduct the pilot program under subsections (a) through (d) shall terminate on the date that is 3 years after the date of enactment of this Act.