.....

(Original Signature of Member)

116TH CONGRESS
1ST 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 in the Cybersecurity and Infrastructure Security Agency of 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 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 Diagnostics and Mitigation Act''.

SEC. 2. ESTABLISHMENT OF 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 of Cybersecurity and Infrastructure Security, shall deploy, operate, and maintain a continuous diagnostics and mitigation program for agencies. Under such program, 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) make program capabilities available for use, with or without reimbursement, to civilian agencies and State, local, Tribal, and territorial governments;

''(iv) employ shared services, collective purchasing, blanket purchase agreements, and any other economic or procurement models the Secretary determines appropriate to maximize the costs savings associated with implementing an information system;

''(v) assist entities in setting information security priorities and assessing and managing cybersecurity risks; and

''(vi) develop policies and procedures for reporting systemic cybersecurity risks and potential incidents based upon data collected under such program.

''(B) REGULAR IMPROVEMENT.—The Secretary shall regularly deploy new technologies and modify existing technologies to the continuous diagnostics and mitigation program required under subparagraph (A), as appropriate, to improve the program.

''(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 the Secretary all infor-

mation, 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 shall, as appropriate—

''(A) share with agencies relevant analysis and products developed under such program;

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

''(C) provide comparative assessments of cybersecurity risks for agencies.''.

(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 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 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 enactment of this Act.

(B) 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.

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

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

(E) Recommendations for using the data collected by such program for creating a common framework for data analytics, visualization of enterprise-wide risks, and real-time report-

ing, and comparative assessments for cybersecurity risks.

(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.

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

(c) REPORT.—Not later than 180 days after the development of the strategy required under subsection (b), the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representative a report on cybersecurity risk posture based on the data collected through the continuous diagnostics and mitigation program under subsection (g) of section 2213 of the Homeland Security Act of 2002 (6 U.S.C. 663), as added by subsection (a).

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

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