117TH CONGRESS
2D SESSION

S. 3863

To require the Secretary of Veterans Affairs to obtain an independent cybersecurity assessment of information systems of the Department of Veterans Affairs, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MARCH 17, 2022

Ms. ROSEN (for herself and Mrs. BLACKBURN) introduced the following bill; which was read twice and referred to the Committee on Veterans' Affairs

---

A BILL

To require the Secretary of Veterans Affairs to obtain an independent cybersecurity assessment of information systems of the Department of Veterans Affairs, 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 ''Strengthening VA Cybersecurity Act of 2022''.

SEC. 2. INDEPENDENT CYBERSECURITY ASSESSMENT OF INFORMATION SYSTEMS OF DEPARTMENT OF VETERANS AFFAIRS.

(a) INDEPENDENT ASSESSMENT REQUIRED.—

(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Veterans Affairs shall enter into an agreement with a federally funded research and development center to provide the Secretary with an independent cybersecurity assessment of—

(A) not more than 10 and not fewer than three high-impact information systems of the Department of Veterans Affairs; and

(B) the effectiveness of the information security program and information security management system of the Department.

(2) DETAILED ANALYSIS.—The independent cybersecurity assessment provided under paragraph (1) shall include a detailed analysis of the ability of the Department—

(A) to ensure the confidentiality, integrity, and availability of the information, information systems, and devices of the Department; and

(B) to protect against—

(i) advanced persistent cybersecurity threats;

(ii) ransomware;

(iii) denial of service attacks;

(iv) insider threats;

(v) threats from foreign actors, including State sponsored criminals and other foreign based criminals;

(vi) phishing;

(vii) credential theft;

(viii) cybersecurity attacks that target the supply chain of the Department;

(ix) threats due to remote access and telework activity; and

(x) other cyber threats.

(3) TYPES OF SYSTEMS.—The independent cybersecurity assessment provided under paragraph (1) shall cover on-premises, remote, cloud-based, and mobile information systems and devices used by, or in support of, Department activities.

(4) SHADOW INFORMATION TECHNOLOGY.—The independent cybersecurity assessment provided under paragraph (1) shall include an evaluation of the use of information technology systems, devices, and services by employees and contractors of the Department who do so without the elements of the Department that are responsible for information tech-

nology at the Department knowing or approving of such use.

(5) METHODOLOGY.—In conducting the cybersecurity assessment provided under paragraph (1), the federally funded research and development center shall take into account industry best practices and the current state-of-the-art in cybersecurity evaluation and review.

(b) PLAN.—

(1) IN GENERAL.—Not later than 120 days after the date on which an independent assessment is provided to the Secretary pursuant to an agreement entered into under subsection (a) with a federally funded research and development center, the Secretary shall submit to Congress a plan to address the findings of the federally funded research and development center set forth in such assessment.

(2) ELEMENTS.—The plan submitted under paragraph (1) shall include the following:

(A) A cost estimate for implementing the plan.

(B) A timeline for implementing the plan.

(C) Such other elements as the Secretary considers appropriate.

(c) COMPTROLLER GENERAL OF THE UNITED STATES REVIEW.—Not later than 180 days after the date of the submission of the plan under (b)(1), the Comptroller General of the United States shall—

(1) commence a review of—

(A) the independent cybersecurity assessment provided under subsection (a); and

(B) the response of the Department to such assessment; and

(2) submit to Congress a report of the results of that review commenced under paragraph (1), including any recommendations made to the Secretary regarding the matters covered by the report.

○