

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.

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 “Strengthening VA Cy-
5 bersecurity Act of 2022”.

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

4 (a) INDEPENDENT ASSESSMENT REQUIRED.—

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

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

14 (B) the effectiveness of the information se-
15 curity program and information security man-
16 agement system of the Department.

17 (2) DETAILED ANALYSIS.—The independent cy-
18 bersecurity assessment provided under paragraph
19 (1) shall include a detailed analysis of the ability of
20 the Department—

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

24 (B) to protect against—

25 (i) advanced persistent cybersecurity
26 threats;

- 1 (ii) ransomware;
- 2 (iii) denial of service attacks;
- 3 (iv) insider threats;
- 4 (v) threats from foreign actors, in-
- 5 cluding State sponsored criminals and
- 6 other foreign based criminals;
- 7 (vi) phishing;
- 8 (vii) credential theft;
- 9 (viii) cybersecurity attacks that target
- 10 the supply chain of the Department;
- 11 (ix) threats due to remote access and
- 12 telework activity; and
- 13 (x) other cyber threats.

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

19 (4) SHADOW INFORMATION TECHNOLOGY.—The
20 independent cybersecurity assessment provided
21 under paragraph (1) shall include an evaluation of
22 the use of information technology systems, devices,
23 and services by employees and contractors of the De-
24 partment who do so without the elements of the De-
25 partment 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.

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

5 (1) commence a review of—

6 (A) the independent cybersecurity assess-
7 ment provided under subsection (a); and

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

10 (2) submit to Congress a report of the results
11 of that review commenced under paragraph (1), in-
12 cluding any recommendations made to the Secretary
13 regarding the matters covered by the report.

○