Strengthening VA Cybersecurity Act of 2022

[Public Law 117–302]

[This law has not been amended]

[Currency: This publication is a compilation of the text of Public Law 117-302. It was last amended by the public law listed in the As Amended Through note above and below at the bottom of each page of the pdf version and reflects current law through the date of the enactment of the public law listed at https://www.govinfo.gov/app/collection/comps/]

[Note: While this publication does not represent an official version of any Federal statute, substantial efforts have been made to ensure the accuracy of its contents. The official version of Federal law is found in the United States Statutes at Large and in the United States Code. The legal effect to be given to the Statutes at Large and the United States Code is established by statute (1 U.S.C. 112, 204).]

AN ACT 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" or the "SVAC 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 seek to enter into an agreement with a federally funded research and development center to provide to the Secretary an independent cybersecurity assessment of—

(A) five 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 heads of the elements of the Department that are responsible for information technology at the Department knowing or approving of such use.

(5) METHODOLOGY.—In conducting the cybersecurity assessment to be 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 by a federally funded research and development center pursuant to an agreement entered into under subsection (a), the Secretary shall submit to the Committees on Veterans' Affairs of the House of Representatives and the Senate 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) Improvements to the security controls of the information systems of the Department assessed under subsection (a) to—

(i) achieve the goals specified in subparagraph (A) of paragraph (2) of such subsection; and

(ii) protect against the threats specified in subparagraph (B) of such paragraph.

(B) Improvements to the information security program and information security management system of the Department to achieve such goals and protect against such threats.

(C) A cost estimate for implementing the plan.

(D) A timeline for implementing the plan.

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

(c) COMPTROLLER GENERAL OF THE UNITED STATES EVALUATION AND REVIEW.—Not later than 180 days after the date of the

submission of the plan under subsection (b)(1), the Comptroller General of the United States shall—

(1) commence an evaluation and review of—

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

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

(2) provide to the Committees on Veterans' Affairs of the House of Representatives and the Senate a briefing on the results of the evaluation and review, including any recommendations made to the Secretary regarding the matters covered by the briefing.