I

119TH CONGRESS
1ST SESSION

H. R. 872

To require covered contractors implement a vulnerability disclosure policy consistent with NIST guidelines, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 31, 2025

Ms. MACE (for herself and Ms. BROWN) introduced the following bill; which was referred to the Committee on Oversight and Government Reform, and in addition to the Committee on Armed Services, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To require covered contractors implement a vulnerability disclosure policy consistent with NIST guidelines, 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 ''Federal Contractor Cybersecurity Vulnerability Reduction Act of 2025''.

SEC. 2. FEDERAL CONTRACTOR VULNERABILITY DISCLOSURE POLICY.

(a) RECOMMENDATIONS.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of the Office of Management and Budget, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, the Director of the National Institute of Standards and Technology, and any other appropriate head of an Executive department, shall—

(A) review the Federal Acquisition Regulation contract requirements and language for contractor vulnerability disclosure programs; and

(B) recommend updates to such requirements and language to the Federal Acquisition Regulation Council.

(2) CONTENTS.—The recommendations required by paragraph (1) shall include updates to such requirements designed to ensure that covered contractors implement a vulnerability disclosure policy consistent with NIST guidelines for contractors as required under section 5 of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3c; Public Law 116–207).

(b) PROCUREMENT REQUIREMENTS.—Not later than 180 days after the date on which the recommended contract language developed pursuant to subsection (a) is received, the Federal Acquisition Regulation Council shall review the recommended contract language and update the FAR as necessary to incorporate requirements for covered contractors to receive information about a potential security vulnerability relating to an information system owned or controlled by a contractor, in performance of the contract.

(c) ELEMENTS.—The update to the FAR pursuant to subsection (b) shall—

(1) to the maximum extent practicable, align with the security vulnerability disclosure process and coordinated disclosure requirements relating to Federal information systems under sections 5 and 6 of the IoT Cybersecurity Improvement Act of 2020 (Public Law 116–207; 15 U.S.C. 278g–3c and 278g–3d); and

(2) to the maximum extent practicable, be aligned with industry best practices and Standards 29147 and 30111 of the International Standards Organization (or any successor standard) or any other appropriate, relevant, and widely used standard.

(d) WAIVER.—The head of an agency may waive the security vulnerability disclosure policy requirement under subsection (b) if—

(1) the agency Chief Information Officer determines that the waiver is necessary in the interest of national security or research purposes; and

(2) if, not later than 30 days after granting a waiver, such head submits a notification and justification (including information about the duration of the waiver) to the Committee on Oversight and Government Reform of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

(e) DEPARTMENT OF DEFENSE SUPPLEMENT TO THE FEDERAL ACQUISITION REGULATION.—

(1) REVIEW.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall review the Department of Defense Supplement to the Federal Acquisition Regulation contract requirements and language for contractor vulnerability disclosure programs and develop updates to such requirements designed to ensure that covered contractors implement a vulnerability disclosure policy consistent with NIST guidelines for contractors as required under section 5 of the IoT Cy-

bersecurity Improvement Act of 2020 (15 U.S.C. 278g–3c; Public Law 116–207).

(2) REVISIONS.—Not later than 180 days after the date on which the review required under subsection (a) is completed, the Secretary shall revise the DFARS as necessary to incorporate requirements for covered contractors to receive information about a potential security vulnerability relating to an information system owned or controlled by a contractor, in performance of the contract.

(3) ELEMENTS.—The Secretary shall ensure that the revision to the DFARS described in this subsection is carried out in accordance with the requirements of paragraphs (1) and (2) of subsection (c).

(4) WAIVER.—The Chief Information Officer of the Department of Defense may waive the security vulnerability disclosure policy requirements under paragraph (2) if the Chief Information Officer—

(A) determines that the waiver is necessary in the interest of national security or research purposes; and

(B) not later than 30 days after granting a waiver, submits a notification and justification (including information about the duration

of the waiver) to the Committees on Armed Services of the House of Representatives and the Senate.

(f) DEFINITIONS.—In this section:

(1) The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(2) The term ''covered contractor'' means a contractor (as defined in section 7101 of title 41, United States Code)—

(A) whose contract is in an amount the same as or greater than the simplified acquisition threshold; or

(B) that uses, operates, manages, or maintains a Federal information system (as defined by section 11331 of title 40, United Stated Code) on behalf of an agency.

(3) The term ''DFARS'' means the Department of Defense Supplement to the Federal Acquisition Regulation.

(4) The term ''Executive department'' has the meaning given that term in section 101 of title 5, United States Code.

(5) The term ''FAR'' means the Federal Acquisition Regulation.

(6) The term ''NIST'' means the National Institute of Standards and Technology.

(7) The term ''OMB'' means the Office of Management and Budget.

(8) The term ''security vulnerability'' has the meaning given that term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(9) The term ''simplified acquisition threshold'' has the meaning given that term in section 134 of title 41, United States Code.

○