

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.

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 “Federal Contractor
5 Cybersecurity Vulnerability Reduction Act of 2025”.

6 **SEC. 2. FEDERAL CONTRACTOR VULNERABILITY DISCLO-**
7 **SURE POLICY.**

8 (a) RECOMMENDATIONS.—

1 (1) IN GENERAL.—Not later than 180 days
2 after the date of the enactment of this Act, the Di-
3 rector of the Office of Management and Budget, in
4 consultation with the Director of the Cybersecurity
5 and Infrastructure Security Agency, the National
6 Cyber Director, the Director of the National Insti-
7 tute of Standards and Technology, and any other
8 appropriate head of an Executive department,
9 shall—

10 (A) review the Federal Acquisition Regula-
11 tion contract requirements and language for
12 contractor vulnerability disclosure programs;
13 and

14 (B) recommend updates to such require-
15 ments and language to the Federal Acquisition
16 Regulation Council.

17 (2) CONTENTS.—The recommendations re-
18 quired by paragraph (1) shall include updates to
19 such requirements designed to ensure that covered
20 contractors implement a vulnerability disclosure pol-
21 icy consistent with NIST guidelines for contractors
22 as required under section 5 of the IoT Cybersecurity
23 Improvement Act of 2020 (15 U.S.C. 278g–3c; Pub-
24 lic Law 116–207).

1 (b) PROCUREMENT REQUIREMENTS.—Not later than
2 180 days after the date on which the recommended con-
3 tract language developed pursuant to subsection (a) is re-
4 ceived, the Federal Acquisition Regulation Council shall
5 review the recommended contract language and update the
6 FAR as necessary to incorporate requirements for covered
7 contractors to receive information about a potential secu-
8 rity vulnerability relating to an information system owned
9 or controlled by a contractor, in performance of the con-
10 tract.

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

13 (1) to the maximum extent practicable, align
14 with the security vulnerability disclosure process and
15 coordinated disclosure requirements relating to Fed-
16 eral information systems under sections 5 and 6 of
17 the IoT Cybersecurity Improvement Act of 2020
18 (Public Law 116–207; 15 U.S.C. 278g–3c and
19 278g–3d); and

20 (2) to the maximum extent practicable, be
21 aligned with industry best practices and Standards
22 29147 and 30111 of the International Standards
23 Organization (or any successor standard) or any
24 other appropriate, relevant, and widely used stand-
25 ard.

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

4 (1) the agency Chief Information Officer deter-
5 mines that the waiver is necessary in the interest of
6 national security or research purposes; and

7 (2) if, not later than 30 days after granting a
8 waiver, such head submits a notification and jus-
9 tification (including information about the duration
10 of the waiver) to the Committee on Oversight and
11 Government Reform of the House of Representatives
12 and the Committee on Homeland Security and Gov-
13 ernmental Affairs of the Senate.

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

16 (1) REVIEW.—Not later than 180 days after
17 the date of the enactment of this Act, the Secretary
18 of Defense shall review the Department of Defense
19 Supplement to the Federal Acquisition Regulation
20 contract requirements and language for contractor
21 vulnerability disclosure programs and develop up-
22 dates to such requirements designed to ensure that
23 covered contractors implement a vulnerability disclo-
24 sure policy consistent with NIST guidelines for con-
25 tractors 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

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

4 (f) DEFINITIONS.—In this section:

5 (1) The term “agency” has the meaning given
6 the term in section 3502 of title 44, United States
7 Code.

8 (2) The term “covered contractor” means a
9 contractor (as defined in section 7101 of title 41,
10 United States Code)—

11 (A) whose contract is in an amount the
12 same as or greater than the simplified acquisi-
13 tion threshold; or

14 (B) that uses, operates, manages, or main-
15 tains a Federal information system (as defined
16 by section 11331 of title 40, United States
17 Code) on behalf of an agency.

18 (3) The term “DFARS” means the Department
19 of Defense Supplement to the Federal Acquisition
20 Regulation.

21 (4) The term “Executive department” has the
22 meaning given that term in section 101 of title 5,
23 United States Code.

24 (5) The term “FAR” means the Federal Acqui-
25 sition Regulation.

1 (6) The term “NIST” means the National In-
2 stitute of Standards and Technology.

3 (7) The term “OMB” means the Office of Man-
4 agement and Budget.

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

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

○