

119TH CONGRESS
1ST SESSION

H. R. 872

IN THE SENATE OF THE UNITED STATES

MARCH 4, 2025

Received; read twice and referred to the Committee on Homeland Security and
Governmental Affairs

AN ACT

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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Federal Contractor
3 Cybersecurity Vulnerability Reduction Act of 2025”.

4 **SEC. 2. FEDERAL CONTRACTOR VULNERABILITY DISCLO-**
5 **SURE POLICY.**

6 (a) RECOMMENDATIONS.—

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

16 (A) review the Federal Acquisition Regula-
17 tion contract requirements and language for
18 contractor vulnerability disclosure programs;
19 and

20 (B) recommend updates to such require-
21 ments and language to the Federal Acquisition
22 Regulation Council.

23 (2) CONTENTS.—The recommendations re-
24 quired by paragraph (1) shall include updates to
25 such requirements designed to ensure that covered
26 contractors implement a vulnerability disclosure pol-

1 icy consistent with NIST guidelines for contractors
2 as required under section 5 of the IoT Cybersecurity
3 Improvement Act of 2020 (15 U.S.C. 278g–3c; Pub-
4 lic Law 116–207).

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

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

17 (1) to the maximum extent practicable, align
18 with the security vulnerability disclosure process and
19 coordinated disclosure requirements relating to Fed-
20 eral information systems under sections 5 and 6 of
21 the IoT Cybersecurity Improvement Act of 2020
22 (Public Law 116–207; 15 U.S.C. 278g–3c and
23 278g–3d); and

24 (2) to the maximum extent practicable, be
25 aligned with industry best practices and Standards

1 29147 and 30111 of the International Standards
2 Organization (or any successor standard) or any
3 other appropriate, relevant, and widely used stand-
4 ard.

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

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

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

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

20 (1) REVIEW.—Not later than 180 days after
21 the date of the enactment of this Act, the Secretary
22 of Defense shall review the Department of Defense
23 Supplement to the Federal Acquisition Regulation
24 contract requirements and language for contractor
25 vulnerability disclosure programs and develop up-

1 dates to such requirements designed to ensure that
2 covered contractors implement a vulnerability disclo-
3 sure policy consistent with NIST guidelines for con-
4 tractors as required under section 5 of the IoT Cy-
5 bersecurity Improvement Act of 2020 (15 U.S.C.
6 278g–3c; Public Law 116–207).

7 (2) REVISIONS.—Not later than 180 days after
8 the date on which the review required under sub-
9 section (a) is completed, the Secretary shall revise
10 the DFARS as necessary to incorporate require-
11 ments for covered contractors to receive information
12 about a potential security vulnerability relating to an
13 information system owned or controlled by a con-
14 tractor, in performance of the contract.

15 (3) ELEMENTS.—The Secretary shall ensure
16 that the revision to the DFARS described in this
17 subsection is carried out in accordance with the re-
18 quirements of paragraphs (1) and (2) of subsection
19 (c).

20 (4) WAIVER.—The Chief Information Officer of
21 the Department of Defense, in consultation with the
22 National Manager for National Security Systems,
23 may waive the security vulnerability disclosure policy
24 requirements under paragraph (2) if the Chief Infor-
25 mation Officer—

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

4 (B) not later than 30 days after granting
5 a waiver, submits a notification and justifica-
6 tion (including information about the duration
7 of the waiver) to the Committees on Armed
8 Services of the House of Representatives and
9 the Senate.

10 (f) DEFINITIONS.—In this section:

11 (1) The term “agency” has the meaning given
12 the term in section 3502 of title 44, United States
13 Code.

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

17 (A) whose contract is in an amount the
18 same as or greater than the simplified acquisi-
19 tion threshold; or

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

1 (3) The term “DFARS” means the Department
2 of Defense Supplement to the Federal Acquisition
3 Regulation.

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

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

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

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

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

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

Passed the House of Representatives March 3,
2025.

Attest: KEVIN F. MCCUMBER,
Clerk.