

**Suspend the Rules and Pass the Bill, H.R. 872, with An Amendment**

**(The amendment strikes all after the enacting clause and inserts a new text)**

119<sup>TH</sup> CONGRESS  
1<sup>ST</sup> 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”.

1 **SEC. 2. FEDERAL CONTRACTOR VULNERABILITY DISCLO-**  
2 **SURE POLICY.**

3 (a) RECOMMENDATIONS.—

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

13 (A) review the Federal Acquisition Regula-  
14 tion contract requirements and language for  
15 contractor vulnerability disclosure programs;  
16 and

17 (B) recommend updates to such require-  
18 ments and language to the Federal Acquisition  
19 Regulation Council.

20 (2) CONTENTS.—The recommendations re-  
21 quired by paragraph (1) shall include updates to  
22 such requirements designed to ensure that covered  
23 contractors implement a vulnerability disclosure pol-  
24 icy consistent with NIST guidelines for contractors  
25 as required under section 5 of the IoT Cybersecurity

1 Improvement Act of 2020 (15 U.S.C. 278g–3c; Pub-  
2 lic Law 116–207).

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

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

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

22 (2) to the maximum extent practicable, be  
23 aligned with industry best practices and Standards  
24 29147 and 30111 of the International Standards  
25 Organization (or any successor standard) or any

1 other appropriate, relevant, and widely used stand-  
2 ard.

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

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

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

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

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

1       sure policy consistent with NIST guidelines for con-  
2       tractors as required under section 5 of the IoT Cy-  
3       bersecurity Improvement Act of 2020 (15 U.S.C.  
4       278g–3c; Public Law 116–207).

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

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

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