



(Original Signature of Member)

118TH CONGRESS
1ST SESSION

H. R. _____

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

IN THE HOUSE OF REPRESENTATIVES

Ms. MACE introduced the following bill; which was referred to the Committee on _____

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 Cybersecurity
5 Vulnerability Reduction Act of 2023”.

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

3 (a) **IN GENERAL.**—Not later than 180 days after
4 the date of the enactment of this Act, the Director of the
5 Office of Management and Budget, in consultation with
6 the Director of the Cybersecurity and Infrastructure Secu-
7 rity Agency, the National Cyber Director, the Director of
8 the National Institute of Standards and Technology, and
9 any other appropriate head of an Executive department,
10 shall review the Federal Acquisition Regulation contract
11 requirements and language for contractor vulnerability
12 disclosure programs and recommend updates to such re-
13 quirements and language to the Federal Acquisition Regu-
14 lation Council. The recommendations shall include up-
15 dates to such requirements designed to ensure that cov-
16 ered contractors implement a vulnerability disclosure pol-
17 icy consistent with NIST guidelines for contractors as re-
18 quired under section 5 of the IoT Cybersecurity Improve-
19 ment Act of 2020 (15 U.S.C. 278g-3c; Public Law 116-
20 207).

21 (b) **PROCUREMENT REQUIREMENTS.**—Not later than
22 60 days after the date on which the recommended contract
23 language developed pursuant to subsection (a) is received,
24 the FAR Council shall review the recommended contract
25 language and update the FAR as necessary to incorporate
26 requirements for covered contractors to receive informa-

1 tion about a potential security vulnerability relating to an
2 information system owned or controlled by a contractor.

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

5 (1) to the maximum extent practicable, be
6 aligned with the NIST guidelines and OMB imple-
7 mentation for contractors as required under sections
8 5 and 6 of the IoT Cybersecurity Improvement Act
9 of 2020 (Public Law 116-207; 15 U.S.C. 278g-3c
10 and 278g-3d);

11 (2) to the maximum extent practicable, be
12 aligned with industry best practices and Standards
13 29147 and 30111 of the International Standards
14 Organization (or any successor standard) or any
15 other appropriate, relevant, and widely-used stand-
16 ard; and

17 (3) not apply to contractors whose contracts are
18 in amounts not greater than the simplified acquisi-
19 tion threshold.

20 (d) WAIVER.—Consistent with section 7(b) of the IoT
21 Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g-
22 3e(b)), the Chief Information Officer of an Executive de-
23 partment may waive the vulnerability disclosure policy re-
24 quirement under subsection (b) if the Chief Information

1 Officer determines that the waiver is necessary in the in-
2 terest of national security or research purposes.

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

5 (1) REVIEW.—Not later than 180 days after
6 the date of the enactment of this Act, the Secretary
7 of Defense shall review the Department of Defense
8 Supplement to the Federal Acquisition Regulation
9 contract requirements and language for contractor
10 vulnerability disclosure programs and develop up-
11 dates to such requirements designed to ensure that
12 covered contractors implement a vulnerability disclo-
13 sure policy consistent with NIST guidelines for con-
14 tractors as required under section 5 of the IoT Cy-
15 bersecurity Improvement Act of 2020 (15 U.S.C.
16 278g-3e; Public Law 116-207).

17 (2) REVISIONS.—Not later than 60 days after
18 the date on which the review required under sub-
19 section (a) is completed, the Secretary shall revise
20 the DFARS as necessary to incorporate require-
21 ments for covered contractors to receive information
22 about a potential security vulnerability relating to an
23 information system owned or controlled by a con-
24 tractor.

1 (3) ELEMENTS.—The Secretary shall ensure
2 that the revision to the DFARS described in this
3 subsection is carried out in accordance with the re-
4 quirements of paragraphs (1), (2), and (3) of sub-
5 section (c).

6 (4) WAIVER.—The Chief Information Officer of
7 the Department of Defense may waive the security
8 vulnerability disclosure requirements under para-
9 graph (2) if the Chief Information Officer deter-
10 mines that the waiver is necessary in the interest of
11 national security or research purposes.

12 (f) DEFINITIONS.—In this section:

13 (1) COVERED CONTRACTOR.—The term “cov-
14 ered contractor” means a contractor (as defined in
15 section 7101 of title 41, United States Code) whose
16 contract is in an amount the same as or greater
17 than the simplified acquisition threshold.

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

21 (3) EXECUTIVE DEPARTMENT.—The term “Ex-
22 ecutive department” has the meaning given that
23 term in section 101 of title 5, United States Code.

24 (4) FAR.—The term “FAR” means the Fed-
25 eral Acquisition Regulation.

1 (5) NIST.—The term “NIST” means the Na-
2 tional Institute of Standards and Technology.

3 (6) OMB.—The term “OMB” means the Office
4 of Management and Budget.

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

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