

**AMENDMENT IN THE NATURE OF A SUBSTITUTE
TO H.R. 5255
OFFERED BY MR. COMER OF KENTUCKY**

Strike all after the enacting clause and insert the following:

1 SECTION 1. SHORT TITLE.

2 This Act may be cited as the “Federal Contractor
3 Cybersecurity Vulnerability Reduction Act of 2024”.

**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

1 contractor vulnerability disclosure programs;
2 and

3 (B) recommend updates to such require-
4 ments and language to the Federal Acquisition
5 Regulation Council.

6 (2) CONTENTS.—The recommendations re-
7 quired by paragraph (1) shall include updates to
8 such requirements designed to ensure that covered
9 contractors implement a vulnerability disclosure pol-
10 icy consistent with NIST guidelines for contractors
11 as required under section 5 of the IoT Cybersecurity
12 Improvement Act of 2020 (15 U.S.C. 278g–3c; Pub-
13 lic Law 116–207).

14 (b) PROCUREMENT REQUIREMENTS.—Not later than
15 180 days after the date on which the recommended con-
16 tract language developed pursuant to subsection (a) is re-
17 ceived, the Federal Acquisition Regulation Council shall
18 review the recommended contract language and update the
19 FAR as necessary to incorporate requirements for covered
20 contractors to receive information about a potential secu-
21 rity vulnerability relating to an information system owned
22 or controlled by a contractor, in performance of the con-
23 tract.

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

1 (1) to the maximum extent practicable, align
2 with the security vulnerability disclosure process and
3 coordinated disclosure requirements relating to Fed-
4 eral information systems under sections 5 and 6 of
5 the IoT Cybersecurity Improvement Act of 2020
6 (Public Law 116–207; 15 U.S.C. 278g–3c and
7 278g–3d); and

8 (2) to the maximum extent practicable, be
9 aligned with industry best practices and Standards
10 29147 and 30111 of the International Standards
11 Organization (or any successor standard) or any
12 other appropriate, relevant, and widely used stand-
13 ard.

14 (d) WAIVER.—The head of an agency may waive the
15 security vulnerability disclosure policy requirement under
16 subsection (b) if the agency Chief Information Officer de-
17 termines that the waiver is necessary in the interest of
18 national security or research purposes.

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

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

1 vulnerability disclosure programs and develop up-
2 dates to such requirements designed to ensure that
3 covered contractors implement a vulnerability disclo-
4 sure policy consistent with NIST guidelines for con-
5 tractors as required under section 5 of the IoT Cy-
6 bersecurity Improvement Act of 2020 (15 U.S.C.
7 278g–3c; Public Law 116–207).

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

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

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

1 mines that the waiver is necessary in the interest of
2 national security or research purposes.

3 (f) DEFINITIONS.—In this section:

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

7 (2) COVERED CONTRACTOR.—The term “cov-
8 ered contractor” means a contractor (as defined in
9 section 7101 of title 41, United States Code)—

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

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

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

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

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

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

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

5 (8) 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 (9) 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.

