

Calendar No. 740

118TH CONGRESS
2D SESSION

S. 5028

[Report No. 118–320]

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

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 11, 2024

Mr. WARNER (for himself and Mr. LANKFORD) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

DECEMBER 19 (legislative day, DECEMBER 16), 2024

Reported by Mr. PETERS, with an amendment

[Strike out all after the enacting clause and insert the part printed in *italic*]

A BILL

To require Federal contractors to 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 2024”.

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 (FAR) contract requirements and language
15 for 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 National Institute of Standards
25 and Technology (NIST) guidelines for contractors as

1 required under section 5 of the IoT Cybersecurity
2 Improvement Act of 2020 (15 U.S.C. 278g-3e).

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 amend the
8 FAR as necessary to incorporate requirements for covered
9 contractors to solicit and address information about poten-
10 tial security vulnerabilities relating to an information sys-
11 tem owned or controlled by the contractor that is used
12 in performance of a Federal contract.

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 (15
20 U.S.C. 278g-3e, 278g-3d); and

21 (2) to the maximum extent practicable, be
22 aligned with industry best practices and Standards
23 29147 and 30111 of the International Standards
24 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 the agency Chief Information Officer—

6 (1) determines that the waiver is necessary in
7 the interest of national security or research pur-
8 poses; and

9 (2) not later than 30 days after granting the
10 waiver, submits a notification and justification, in-
11 cluding information about the duration of the waiv-
12 er, to the Committee on Homeland Security and
13 Governmental Affairs of the Senate and the Com-
14 mittee on Oversight and Accountability of the House
15 of Representatives.

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 (DFARS) contract requirements and language for
23 contractor vulnerability disclosure programs and de-
24 velop updates to such requirements designed to en-
25 sure that covered contractors, to the maximum ex-

1 tent practicable, align with the security vulnerability
2 disclosure process and coordinated disclosure re-
3 quirements relating to Federal information systems
4 under sections 5 and 6 of the IoT Cybersecurity Im-
5 provement Act of 2020 (15 U.S.C. 278g-3e, 278g-
6 3d).

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 may waive the security
22 vulnerability disclosure policy requirements under
23 paragraph (2) if the Chief Information 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 the waiver, submits a notification and justifica-
6 tion, including information about the duration
7 of the waiver, to the Committee on Armed Serv-
8 ices of the Senate and the Committee on Armed
9 Services of the House of Representatives.

10 (f) DEFINITIONS.—In this section:

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

14 (2) COVERED CONTRACTOR.—The term “cov-
15 ered contractor” means a contractor (as defined in
16 section 7101 of title 41, 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) EXECUTIVE DEPARTMENT.—The term “Ex-
2 ecutive department” has the meaning given that
3 term in section 101 of title 5, United States Code.

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

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

12 **SECTION 1. SHORT TITLE.**

13 *This Act may be cited as the “Federal Contractor Cy-*
14 *bersecurity Vulnerability Reduction Act of 2024”.*

15 **SEC. 2. FEDERAL CONTRACTOR VULNERABILITY DISCLO-**
16 **SURE POLICY.**

17 (a) RECOMMENDATIONS.—

18 (1) IN GENERAL.—*Not later than 180 days after*
19 *the date of the enactment of this Act, the Director of*
20 *the Office of Management and Budget, in consultation*
21 *with the Director of the Cybersecurity and Infrastruc-*
22 *ture Security Agency, the National Cyber Director,*
23 *the Director of the National Institute of Standards*
24 *and Technology, and any other appropriate head of*
25 *an Executive department, shall—*

1 (A) review the Federal Acquisition Regula-
2 tion (FAR) contract requirements and language
3 for contractor vulnerability disclosure programs;
4 and

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

8 (2) CONTENTS.—The recommendations required
9 by paragraph (1) shall include updates to such re-
10 quirements designed to ensure that covered contractors
11 implement a vulnerability disclosure policy consistent
12 with National Institute of Standards and Technology
13 (NIST) guidelines for contractors as required under
14 section 5 of the IoT Cybersecurity Improvement Act
15 of 2020 (15 U.S.C. 278g–3c).

16 (b) PROCUREMENT REQUIREMENTS.—Not later than
17 180 days after the date on which the recommended contract
18 language developed pursuant to subsection (a) is received,
19 the Federal Acquisition Regulation Council shall review the
20 recommended contract language and amend the FAR as
21 necessary to incorporate requirements for covered contrac-
22 tors to solicit and address information about potential secu-
23 rity vulnerabilities relating to an information system
24 owned or controlled by the contractor that is used in per-
25 formance of a Federal contract.

1 (c) *ELEMENTS.*—*The update to the FAR pursuant to*
2 *subsection (b) shall—*

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

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

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—*

17 (1) *determines that the waiver is necessary in*
18 *the interest of national security or research purposes;*
19 *and*

20 (2) *not later than 30 days after granting the*
21 *waiver, submits a notification and justification, in-*
22 *cluding information about the duration of the waiver,*
23 *to the Committee on Homeland Security and Govern-*
24 *mental Affairs of the Senate and the Committee on*

1 *Oversight and Accountability of the House of Rep-*
2 *resentatives.*

3 *(e) DEFINITIONS.—In this section:*

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

7 *(2) COVERED CONTRACTOR.—The term “covered*
8 *contractor” means a contractor (as defined in section*
9 *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 Code)*
16 *on behalf of an agency.*

17 *(3) EXECUTIVE DEPARTMENT.—The term “Exec-*
18 *utive department” has the meaning given that term*
19 *in section 101 of title 5, United States Code.*

20 *(4) SECURITY VULNERABILITY.—The term “secu-*
21 *rity vulnerability” has the meaning given that term*
22 *in section 2200 of the Homeland Security Act of 2002*
23 *(6 U.S.C. 650).*

24 *(5) SIMPLIFIED ACQUISITION THRESHOLD.—The*
25 *term “simplified acquisition threshold” has the mean-*

1 *ing given that term in section 134 of title 41, United*
2 *States Code.*

3 **SEC. 3. NO ADDITIONAL FUNDING.**

4 *No additional funds are authorized to be appropriated*
5 *for the purpose of carrying out this Act.*

Calendar No. 740

118TH CONGRESS
2^D SESSION

S. 5028

[Report No. 118-320]

A BILL

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

DECEMBER 19 (legislative day, DECEMBER 16), 2024

Reported with an amendment