I

118TH CONGRESS
1ST SESSION

H. R. 5255

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

IN THE HOUSE OF REPRESENTATIVES

AUGUST 22, 2023

Ms. MACE introduced the following bill; which was referred to the Committee on Oversight and Accountability, 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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Federal Cybersecurity Vulnerability Reduction Act of 2023''.

SEC. 2. FEDERAL CONTRACTOR VULNERABILITY DISCLOSURE POLICY.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of the Office of Management and Budget, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, the Director of the National Institute of Standards and Technology, and any other appropriate head of an Executive department, shall review the Federal Acquisition Regulation contract requirements and language for contractor vulnerability disclosure programs and recommend updates to such requirements and language to the Federal Acquisition Regulation Council. The recommendations shall include updates to such requirements designed to ensure that covered contractors implement a vulnerability disclosure policy consistent with NIST guidelines for contractors as required under section 5 of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3c; Public Law 116–207).

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

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

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

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

(2) to the maximum extent practicable, be aligned with industry best practices and Standards 29147 and 30111 of the International Standards Organization (or any successor standard) or any other appropriate, relevant, and widely used standard; and

(3) not apply to contractors whose contracts are in amounts not greater than the simplified acquisition threshold.

(d) WAIVER.—Consistent with section 7(b) of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3e(b)), the Chief Information Officer of an Executive department may waive the vulnerability disclosure policy requirement under subsection (b) if the Chief Information

Officer determines that the waiver is necessary in the interest of national security or research purposes.

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

(1) REVIEW.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall review the Department of Defense Supplement to the Federal Acquisition Regulation contract requirements and language for contractor vulnerability disclosure programs and develop updates to such requirements designed to ensure that covered contractors implement a vulnerability disclosure policy consistent with NIST guidelines for contractors as required under section 5 of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3c; Public Law 116–207).

(2) REVISIONS.—Not later than 60 days after the date on which the review required under subsection (a) is completed, the Secretary shall revise the DFARS as necessary to incorporate requirements for covered contractors to receive information about a potential security vulnerability relating to an information system owned or controlled by a contractor.

(3) ELEMENTS.—The Secretary shall ensure that the revision to the DFARS described in this subsection is carried out in accordance with the requirements of paragraphs (1), (2), and (3) of subsection (c).

(4) WAIVER.—The Chief Information Officer of the Department of Defense may waive the security vulnerability disclosure requirements under paragraph (2) if the Chief Information Officer determines that the waiver is necessary in the interest of national security or research purposes.

(f) DEFINITIONS.—In this section:

(1) COVERED CONTRACTOR.—The term ''covered contractor'' means a contractor (as defined in section 7101 of title 41, United States Code) whose contract is in an amount the same as or greater than the simplified acquisition threshold.

(2) DFARS.—The term ''DFARS'' means the Department of Defense Supplement to the Federal Acquisition Regulation.

(3) EXECUTIVE DEPARTMENT.—The term ''Executive department'' has the meaning given that term in section 101 of title 5, United States Code.

(4) FAR.—The term ''FAR'' means the Federal Acquisition Regulation.

(5) NIST.—The term ''NIST'' means the National Institute of Standards and Technology.

(6) OMB.—The term ''OMB'' means the Office of Management and Budget.

(7) SECURITY VULNERABILITY.—The term ''security vulnerability'' has the meaning given that term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

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

○