Calendar No. 740

118TH CONGRESS *2d Session*	SENATE	REPORT 118–320

FEDERAL CONTRACTOR CYBERSECURITY VULNERABILITY REDUCTION ACT OF 2024

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 5028

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.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

59–010 WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	RAND PAUL, Kentucky
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	JAMES LANKFORD, Oklahoma
JACKY ROSEN, Nevada	MITT ROMNEY, Utah
JON OSSOFF, Georgia	RICK SCOTT, Florida
RICHARD BLUMENTHAL, Connecticut	JOSH HAWLEY, Missouri
ADAM SCHIFF, California	ROGER MARSHALL, Kansas

DAVID M. WEINBERG, *Staff Director*
ALAN S. KAHN, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
EMILY A. FERGUSON, *Professional Staff Member*
WILLIAM E. HENDERSON III, *Minority Staff Director*
CHRISTINA N. SALAZAR, *Minority Chief Counsel*
ANDREW J. HOPKINS, *Minority Counsel*
MEGAN M. KRYNEN, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 740

118TH CONGRESS *2d Session* | SENATE | REPORT 118–320

FEDERAL CONTRACTOR CYBERSECURITY VULNERABILITY REDUCTION ACT OF 2024

DECEMBER 19 (legislative day, DECEMBER 16), 2024.—Ordered to be printed

Mr. PETERS, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 5028]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 5028) to require Federal contractors to implement a vulnerability disclosure policy consistent with NIST guidelines, and for other purposes, having considered the same, reports favorably thereon with an amendment in the nature of a substitute and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 5028, the *Federal Contractor Cybersecurity Vulnerability Reduction Act of 2024*, requires that the Director of the Office of Management and Budget (OMB) review the Federal Acquisition Regulation (FAR) contract requirements and language for contractor vulnerability disclosure programs and recommend updates to such requirements and language to the Federal Acquisition Regulation Council (FARC), for implementation in the FAR. This bill requires that the updates to the FAR align with the security vulnerability disclosure process and requirements, industry best practices, and appropriate standards. Additionally, the bill allows for heads of

agencies to waive the security vulnerability disclosure policy requirement for national security or research purposes.

II. Background and Need for the Legislation

Federal agencies, private companies, critical infrastructure owners and operators, and organizations across the U.S. currently face a growing threat from foreign adversaries and cybercriminals who are using cyberspace to launch attacks that affect our national security and economy.[1] An increasing number of organizations in the public and private sectors are adopting vulnerability disclosure programs to improve their ability to detect security issues before sensitive data is compromised or service is disrupted.[2] Almost all software includes a number of issues with code, commonly called 'bugs' or 'vulnerabilities', and often, these issues are not discovered until the software is deployed or used. For example, the Heartbleed bug, discovered in 2014 in software that encrypted communications between different computers, enabled users to craft malicious messages that gave them access to websites, user accounts, and the capability to steal Personally Identifiable Information (PII), as well as to compromise patient health records.[3] Security researchers, either through contracts with organizations or regular use of the software, can find these vulnerabilities. Rather than not reporting these vulnerabilities to the organizations or openly posting information on the identified issues and drawing additional attention to an unfixed vulnerability, formal vulnerability disclosure programs or policies (VDP) allow for security researchers to submit technical information directly to companies or organizations on issues with their websites or software programs.[4] VDPs allow for organizations to discretely patch vulnerabilities or mitigate security threats before they can be used by cybercriminals or other threat actors.[5] For the Heartbleed bug, the vulnerability was discovered by researchers and reported to the software organization privately, allowing fixes to be prepared before the discovery was publicly announced. This minimized the amount of damage the bug could do to critical systems.[6]

VDPs have become a security best practice and are recommended by the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration, highlighted in Strategic Objective 3.3 of the National Cybersecurity Strategy, and included in the Cybersecurity and Infrastructure Security Agency (CISA)'s Secure by Design Pledge.[7] VDPs are inte-

---

[1] White House, *National Cybersecurity Strategy March* 2023 (Mar 2023) (www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf).

[2] Consumer Reports, *Who Ya' Gonna Call? Why IoT Companies Should Embrace Vulnerability Disclosure Programs* (July 29, 2024) (innovation.consumerreports.org/who-ya-gonna-call/).

[3] Heartbleed Bug (website) (Accessed December 11, 2024) (heartbleed.com/); *The Heartbleed Bug, Explained*, Vox (May 14, 2015) (www.vox.com/2014/6/19/18076318/heartbleed).

[4] BugCrowd, *Vulnerability Disclosure Program (VDP)* (website) (accessed December 3, 2024) (www.bugcrowd.com/glossary/vulnerability-disclosure-program-vdp/).

[5] *Id.*

[6] Heartbleed Bug (Accessed December 11, 2024) (heartbleed.com/); *The Heartbleed Bug, Explained*, Vox (May 14, 2015) (www.vox.com/2014/6/19/18076318/heartbleed).

[7] National Institute of Standards and Technology, *Recommendations for Federal Vulnerability Disclosure Guidelines*, NIST SP 800 216 (May 2023); National Telecommunications and Information Administration, *Improving Cybersecurity Through Enhanced Vulnerability* Disclosure (December 15, 2016) (blog) (www.ntia.gov/blog/2016/improving-cybersecurity-through-enhanced-vulnerability-disclosure); White House, *National Cybersecurity Strategy March* 2023 (Mar 2023) (www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf);

gral to both the public and private sector because they provide an organized, legal means for security researchers to submit technical information that otherwise may not be found or noticed.[8] This also allows organizations to fix vulnerabilities before they are used in a cyberattack, which could save time spent on remediation of systems and funds spent on operational downtime, and potentially avoid paying fines and expensive cyber recovery services.[9] For example, the Department of Defense's pilot VDP for defense industrial base companies found over 200 vulnerabilities in the first 6 months of the program, potentially saving the companies $300 million in response and recovery costs.[10] In 2023, CISA's VDP for federal agencies catalogued over 2,424 valid vulnerability submissions and remedied 872, including 250 critical vulnerabilities.[11]

OMB required executive branch agencies to implement VDPs in 2020, noting that they are an effective method for obtaining insights on security vulnerabilities and have a high return on investment.[12] However, not all federal agencies require contractors to utilize VDPs. This bill requires OMB to review the FAR for VDP requirements and recommend language requiring contracts to include a VDP. OMB must also recommend updates to the FARC to ensure that contractors implement a VDP consistent with NIST guidelines, international standards, and industry best practices. Additionally, the bill requires the FARC to amend the FAR to allow contractors to request information from federal agencies about potential security vulnerabilities related to systems owned or controlled by the contractor.

III. LEGISLATIVE HISTORY

Senators Mark Warner (D–VA) and James Lankford (R–OK) introduced S. 5028, the *Federal Contractor Cybersecurity Vulnerability Reduction Act of 2024*, on September 11, 2024. The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 5028 at a business meeting on November 20, 2024. At the business meeting, Senator Lankford offered a substitute amendment to the bill along with a modification to the amendment, which removed the requirements of the Department of Defense to review the Department of Defense Supplement to the Federal Acquisition Regulation contract requirements and language. The modification to the substitute amendment also stipulated that no additional funds were authorized for the purpose of carrying out the bill after enactment. The modification to the

---

Cybersecurity and Infrastructure Security Agency, *Secure by Design Pledge* (website) (accessed December 3, 2024) (www.cisa.gov/securebydesign/pledge).

[8] National Telecommunications and Information Administration, *Improving Cybersecurity Through Enhanced Vulnerability* Disclosure (December 15, 2016) (blog) (www.ntia.gov/blog/2016/improving-cybersecurity-through-enhanced-vulnerability-disclosure); BugCrowd, *Vulnerability Disclosure Program (VDP)* (website) (accessed December 3, 2024) (www.bugcrowd.com/glossary/vulnerability-disclosure-program-vdp/).

[9] *Id.*

[10] *DOD Cyber Crime Center's Vulnerability Disclosure Program Racking Up Savings for Industrial Base*, DefenseScoop (October 30, 2024) (defensescoop.com/2024/10/30/dc3-defense-industrial-base-vulnerability-disclosure-program-dib-vdp/).

[11] Cybersecurity and Infrastructure Security Agency, *Vulnerability Disclosure Policy Platform 2023 Annual Report* (September 2024) (www.cisa.gov/sites/default/files/2024-09/Vulnerability%20Disclosure%20Policy%20%28VDP%29%20Platform%202023%20Annual%20Report.pdf).

[12] Office of Management and Budget, *Improving Vulnerability Identification, Management, and Remediation* (M-20-23) (September 2, 2020).

Lankford substitute amendment and the substitute amendment, as modified, were adopted by unanimous consent with Senators Peters, Hassan, Rosen, Ossoff, Blumenthal, Butler, Lankford, and Hawley present.

The bill, amended by the Lankford substitute amendment, as modified, was ordered reported favorably by roll call vote of 8 yeas to 0 nays with Senators Peters, Hassan, Rosen, Ossoff, Blumenthal, Butler, Lankford, and Hawley voting in the affirmative. Senators Carper, Sinema, Romney, and Marshall voted yea by proxy, for the record only, and Senators Paul, Johnson, and Scott, voting in the negative by proxy, for the record only.

IV. Section-by-Section Analysis of the Bill, as Reported

Section 1. Short title

The bill may be cited as the "Federal Contractor Cybersecurity Vulnerability Reduction Act of 2024"

Section 2. Federal contractor vulnerability disclosure policy

Subsection (a) requires that the Director of the Office of Management and Budget, in consultation with the Director of CISA, National Cyber Director, and Director of NIST, not later than 180 days, review the Federal Acquisition Regulation (FAR) and recommend updates to the Federal Acquisition Regulation Council to ensure contractors implement a vulnerability disclosure policy consistent with NIST guidelines.

Subsection (b) requires the FAR to review recommended contract language and address information about potential security vulnerabilities no later than 180 days after receipt.

Subsection (c) outlines that the FAR updates shall align with security vulnerability disclosure process and coordinated disclosure requirements in federal information systems, industry best practices, and international standards.

Subsection (d) provides that heads of agencies may waive the requirement for a VDP for national security or research purposes.

Subsection (e) requires the Secretary of Defense to review the Department of Defense Supplement to the Federal Acquisition Regulation (DFARS) for contractor vulnerability disclosure programs and develop updates to these requirements, within 180 days. Additionally, it allows for revision of DFARS and a waiver of the vulnerability disclosure requirements for national security purposes.

Subsection (f) provides definitions for Agency, covered contractor, executive department, security vulnerability and simplified acquisition threshold.

Section 3. No additional funding

This section requires that no additional funds are authorized to be appropriated for the purpose of carrying out this Act.

V. Evaluation of Regulatory Impact

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's state-

ment that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. Changes in Existing Law Made by the Bill, as Reported

This legislation would make no change in existing law, within the meaning of clauses (a) and (b) of subparagraph 12 of rule XXVI of the Standing Rules of the Senate, because this legislation would not repeal or amend any provision of current law.

○