February 28, 2025

The Honorable Mike Johnson
Speaker, U.S. House of Representatives
Washington, DC 20515

The Honorable John Thune
Majority Leader, U.S. Senate
Washington, DC 20510

The Honorable Hakeem Jeffries
Minority Leader, U.S. House of Representatives
Washington, DC 20515

The Honorable Charles Schumer
Minority Leader, U.S. Senate
Washington, DC 20510

Speaker Johnson, Leader Jeffries, Leader Thune and Leader Schumer:

We, the undersigned organizations, would like to thank Representatives Nancy Mace (R-SC) and Shontel Brown (D-OH) for introducing the Federal Contractor Cybersecurity Vulnerability Reduction Act of 2025.[1] This important legislation is a critical step toward strengthening the cybersecurity resilience of our federal government and its contractors.

Originally introduced in August 2023,[2] the bill has since gained widespread bipartisan backing. It received unanimous approval in the House Committee on Oversight and Accountability in May 2024 with a 42-0 vote and was subsequently incorporated as Section 1747 in the House-passed National Defense Authorization Act (NDAA). The companion bill, S. 5028, was introduced in the Senate by Senators Mark Warner (D-VA) and James Lankford (R-OK).[3] This overwhelming support from both chambers underscores the urgent, national imperative to address critical cybersecurity vulnerabilities across federal systems.

This legislation requires federal contractors to implement a Vulnerability Disclosure Policy (VDP), ensuring they have a structured process to receive and address security vulnerabilities. Contractors, given the vast amount of sensitive data they handle, are prime targets for cyber threats. As a result, the bill ensures all companies contracting with the federal government adhere to security best practices.

The bill builds upon existing policies that have encouraged the adoption of VDPs, promoting a proactive approach to cybersecurity and helping protect critical systems before they can be exploited.

[1] H.R. 872, Federal Contractor Cybersecurity Vulnerability Reduction Act of 2025, 119th Cong., https://www.congress.gov/bill/119th-congress/house-bill/872.

[2] H.R. 5255, Federal Cybersecurity Vulnerability Reduction Act of 2023, 118th Cong., https://www.congress.gov/bill/118th-congress/house-bill/5255

[3] S.5028, Federal Contractor Cybersecurity Vulnerability Reduction Act of 2024, 118th Cong., https://www.congress.gov/index.php/bill/118th-congress/senate-bill/5028.

For example, the bill is consistent with the bipartisan Internet of Things Cybersecurity Improvement Act of 2020, which laid the groundwork for improving the security posture of federal systems by mandating the implementation of VDPs across civilian agencies[4]. Additionally, under the Trump administration in 2020, federal agencies were directed to implement VDP programs under the OMB memorandum M-20-32[5], and the Department of Homeland Security issued Binding Operational Directive 20-01[6] to guide these efforts. The Federal Cybersecurity Vulnerability Reduction Act takes this further by expanding the requirement to federal contractors, ensuring that they align with the same cybersecurity standards as federal agencies.

Furthermore, the bill ensures that contractor VDPs are aligned with guidelines from the National Institute of Standards and Technology (NIST). Additionally, it requires the Office of Management and Budget (OMB), in consultation with NIST, Cybersecurity and Infrastructure Security Agency (CISA), and the National Cyber Director (NCD) to recommend new requirements to the Federal Acquisition Regulation (FAR) Council to mandate that contractors implement VDP programs as part of their cybersecurity obligations. The bill also directs the Secretary of Defense to update the Defense Federal Acquisition Regulation (DFAR) to require defense contractors to adopt similar policies.

The legislation specifically exempts contracts under the simplified acquisition threshold, unless the contractor uses, operates, or manages a federal information system on behalf of an agency, and provides a waiver for adopting VDPs in the interest of national security and research purposes.

We are encouraged by the bipartisan support this legislation has received thus far, and we urge the House to swiftly pass it, with the Senate following suit. Strengthening cybersecurity is a strategic priority for this Administration to outpace and outmaneuver our adversaries. By implementing a simple and effective approach to identifying vulnerabilities, we can stay ahead of emerging threats and better protect critical systems.

*   *   *

Sincerely,

HackerOne
Bugcrowd
Infoblox
Microsoft
Rapid7
Schneider Electric
Tenable

[4] Public Law No: 116-207, https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.pdf.

[5] OMB memorandum 20-32, https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf

[6] DHS BOD 20-01, https://www.cisa.gov/news-events/directives/bod-20-01-develop-and-publish-vulnerability-disclosure-policy

Trend Micro