November 13, 2025

The Honorable Mike Rogers
Chairman, House Armed Services Committee
Washington, DC 20515

The Honorable Roger F. Wicker
Chairman, Senate Committee on Armed Services
Washington, DC 20515

The Honorable Adam Smith
Ranking Member, House Armed Services Committee
Washington, DC 20515

The Honorable Jack Reed
Ranking Member, Senate Committee on Armed Services
Washington, DC 20515

Chairman Rogers, Ranking Member Smith, Chairman Wicker, and Ranking Member Reed:

As Congress works to finalize the Fiscal Year 2026 National Defense Authorization Act (NDAA), we, the undersigned organizations, urge you to retain Sec. 1514 of the House-passed bill, which would improve the cybersecurity resilience of the federal government and its contractors. If enacted, this provision would address a longstanding gap in the federal government's cybersecurity defensive posture and ensure contractors are equipped to protect against increasingly sophisticated threats.

Sec. 1514 of the House-passed NDAA enjoys strong bipartisan support in both chambers. It mirrors the language of H.R. 872, the Federal Contractor Cybersecurity Vulnerability Reduction Act of 2025[1], introduced by Reps. Nancy Mace (R-SC) and Shontel Brown (D-OH), which passed the House by voice vote in March. The bipartisan Senate companion bill, S. 1899, was introduced by Sens. Mark Warner (D-VA) and James Lankford (R-OK) in May[2], reflecting shared recognition across party lines that federal contractor security is inseparable from national security.

For years, federal agencies have been required to adopt vulnerability disclosure programs (VDPs), creating a structured process to identify and fix cybersecurity weaknesses. Congress's bipartisan Internet of Things Cybersecurity Improvement Act of 2020[3], along with OMB[4] and DHS directives[5] under the previous Trump administration, demonstrated the value of embedding VDPs into agency operations. Contractors, however, have not been held to this same

[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] S.1899, Federal Contractor Cybersecurity Vulnerability Reduction Act of 2025, 119th Cong. https://www.congress.gov/bill/119th-congress/senate-bill/1899.
[3] Public Law No: 116-207, https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.pdf.
[4] OMB memorandum 20-32, https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf
[5] DHS BOD 20-01, https://www.cisa.gov/news-events/directives/bod-20-01-develop-and-publish-vulnerability-disclosure-policy

cybersecurity standard despite handling vast amounts of sensitive government data and supporting mission-critical systems.

This gap leaves a prime entry point for adversaries seeking to infiltrate federal networks. The Federal Contractor Cybersecurity Vulnerability Reduction Act closes this gap by requiring contractors to implement a VDP as a means to receive and mitigate disclosures of security vulnerabilities in their software and systems before they can be exploited.

Sec. 1514 would ensure that contractor VDPs follow the guidelines established by the National Institute of Standards and Technology (NIST). It also directs the Office of Management and Budget (OMB), in consultation with NIST, the Cybersecurity and Infrastructure Security Agency (CISA), and the National Cyber Director (NCD), to recommend updates to the Federal Acquisition Regulation (FAR) Council. These updates would require contractors to implement VDPs as part of their cybersecurity obligations.

Additionally, Sec. 1514 directs the Secretary of Defense to update the Defense Federal Acquisition Regulation (DFAR) to bring defense contractors into compliance. The provision specifically exempts contracts under the simplified acquisition threshold and allows for waivers when necessary for national security or research purposes.

* * *

There is no doubt that adversaries will continue to probe for weaknesses in the federal supply chain, and contractors remain a target. Extending VDPs to contractors closes a security gap, matures cyber defenses, brings consistency across government and industry, and helps to ensure that vulnerabilities are discovered and fixed before they can be weaponized.

Thank you for your attention to this vital issue. We look forward to working collaboratively with you to advance our shared goal of a safer, more secure cyber environment.

Sincerely,

HackerOne
BugCrowd
Desired Effect
GitHub
Infoblox
Integriti
Microsoft
Rapid7
Schneider Electric
Tenable
Trend Micro
Veeam
Zenity