October 15, 2024

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

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

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

The Honorable Mitch McConnell
Minority Leader, U.S. Senate
Washington, DC 20510

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

As Congress works to finalize the Fiscal Year 2025 National Defense Authorization Act, we urge you to retain Sec. 1747 of the House-passed bill which would improve federal contractor cybersecurity vulnerability disclosure policies. If enacted, this provision would represent a pivotal step forward in bolstering the cybersecurity defenses of federal contractors and, by extension, the national security of the United States.

Sec. 1747 of the House-passed NDAA enjoys strong bipartisan support in both the House and Senate. It mirrors the language of H.R. 5255, the Federal Cybersecurity Vulnerability Reduction Act, introduced by Congresswoman Nancy Mace (R-SC) and approved 42-0 by the Committee on Oversight and Accountability in May and S. 5028, the Federal Contractor Cybersecurity Vulnerability Reduction Act, introduced by Senators Mark Warner (D-VA) and James Lankford (R-OK).

Federal contractors and subcontractors play a crucial role in supporting the government's operations and often handle sensitive government information and personal data. As a result, they are frequent targets for cyberattacks by hackers seeking to exploit vulnerabilities to gain access to government information.

Under Sec. 1747, federal contractors would be required to implement a Vulnerability Disclosure Policy (VDP) as a means to receive disclosures of security vulnerabilities in their software and systems. This would ensure that, despite the continuously evolving threat landscape, contractors are equipped to address security vulnerabilities proactively, implementing necessary patches or other mitigations as needed to protect critical systems before they can be exploited.

Currently, while civilian federal agencies are required to implement Vulnerability Disclosure Programs (VDPs), there is no similar mandate for some federal contractors.[1] Sec. 1747 addresses that gap by building on the existing framework established by the bipartisan Internet of Things Cybersecurity Improvement Act of 2020.[2] It specifically exempts contracts under the simplified acquisition threshold and provides a waiver for adopting VDPs in the interest of national security and research purposes.

In line with the standards set by the Internet of Things Cybersecurity Improvement Act, it ensures that federal contractors are also aligned with guidelines established by the National Institute of Standards and Technology (NIST). It tasks the Office of Management and Budget (OMB), in consultation with NIST, the Cybersecurity and Infrastructure Security Agency (CISA), and the National Cyber Director (NCD), with recommending new requirements to the Federal Acquisition Regulation (FAR) Council. These recommendations would require covered contractors to implement VDPs as part of their cybersecurity obligations.

Additionally, it directs the Secretary of Defense to update the Defense Federal Acquisition Regulation (DFAR) to ensure that covered Defense contractors are also required to implement VDPs. By expanding the requirement to federal contractors, it strengthens the cybersecurity posture of the entire federal supply chain, ensuring that vulnerabilities are proactively identified and addressed across both civilian and defense sectors.

* * *

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
Business Software Alliance (BSA)
Cisco
Cybersecurity Coalition
Google
Hacking Policy Council
Microsoft

---

[1] OMB memorandum 20-32, https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf. DHS BOD 20-01, https://www.cisa.gov/news-events/directives/bod-20-01-develop-and-publish-vulnerability-disclosure-policy.

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

CC:

The Honorable Jack Reed
Chairman,
Senate Armed Services Committee
Washington, DC 20510

The Honorable Roger Wicker
Ranking Member,
Senate Armed Services Committee
Washington, DC 20510

The Honorable Gary Peters
Chairman,
Homeland Security and
Government Affairs Committee
Washington, DC 20510

The Honorable Rand Paul
Ranking Member,
Homeland Security and
Government Affairs Committee
Washington, DC 20510

The Honorable James Comer
Chairman,
House Oversight and
Accountability Committee
Washington, DC 20515

The Honorable Jamie Raskin
Ranking Member,
House Oversight and
Accountability Committee
Washington, DC 20515

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

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