

May 13, 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

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

Speaker Johnson, Leader Jeffries, Leader Schumer, Leader McConnell, Chairman Peters, Ranking Member Paul, Chairman Comer, Ranking Member Raskin, Chairman Rogers, and Ranking Member Smith:

We, the undersigned organizations, urge the prioritization and prompt passage of the Federal Cybersecurity Vulnerability Reduction Act (H.R.5255).¹ We are very pleased to see that the

¹ H.R. 5255, Federal Cybersecurity Vulnerability Reduction Act of 2023, 118th Cong., <https://www.congress.gov/bill/118th-congress/house-bill/5255>.

House Oversight and Accountability Committee has scheduled a markup of H.R. 5255 for May 15, 2024.²

This important legislation would enhance the security of government information systems. Under the bill, federal contractors would implement a Vulnerability Disclosure Program (VDP) as a means to receive disclosures of security vulnerabilities in their software and computers so that the vulnerabilities can be assessed and mitigated. VDPs are a widely accepted cybersecurity best practice that helps system operators address vulnerabilities before cybercriminals exploit them.

H.R.5255 builds on existing requirements and processes of the bipartisan Internet of Things Cybersecurity Improvement Act, which became law in 2020.³ The bill exempts contracts under the simplified acquisition threshold and provides a waiver for national security systems. As under the Internet of Things Cybersecurity Improvement Act of 2020, the bill ensures that contractor VDPs are consistent with National Institute for Standards and Technology (NIST) guidelines. The legislation directs the Office of Management and Budget (OMB), in consultation with the directors of NIST, the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cyber Director (NCD) to recommend new requirements to the Federal Acquisition Regulation Council to require covered contractors to implement VDP programs. Additionally, it directs the Secretary of Defense to develop updates to the Defense Federal Acquisition Regulations to require covered Defense contractors to implement VDP programs.

This proposed legislation takes crucial steps to bolstering the cybersecurity resilience of our nation. In 2020, federal agencies were directed to implement VDP programs through the Office of Management and Budget memorandum M-20-32⁴ and the Department of Homeland Security issued Binding Operational Directive 20-01.⁵ While federal agencies have implemented VDP programs, not all government contractors have adopted VDPs of their own. Federal contractors are an integral part of federal supply chains and infrastructure, and they pose a unique security risk given their proximity to government data and access to government networks. H.R.5255 helps ensure all companies that do business with the federal government are following security best practices to stay ahead of malicious actors, prevent potential exploits, and protect sensitive information.

* * *

² Full Committee on Oversight and Accountability Business Meeting, <https://oversight.house.gov/markup/full-committee-business-meeting-72/>

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>

We appreciate your continued efforts on this important issue and stay ready to collaborate with you to help get this legislation codified into law. Should you have any questions, or if we can assist in any other way, please contact us.

Sincerely,

HackerOne
Bugcrowd
Cisco
GitHub
Google
Intel
Intigriti
Kontent.ai
Mattermost
Microsoft
Okta
onShore Security
Palo Alto Networks
Schneider Electric
Summit V
Rapid7
Tenable
Trend Micro
Zoom