



HACKING POLICY COUNCIL

Comments on the Request for Information on Modernizing the National Vulnerability Database in the Age of Artificial Intelligence

October 13, 2026

The Hacking Policy Council (HPC) respectfully submits the following comments in response to the National Institute of Standards and Technology's (NIST) Request for Information on Modernizing the National Vulnerability Database (NVD) in the Age of Artificial Intelligence (AI).

HPC is a group of experts dedicated to creating a more favorable legal, policy, and business environment for good-faith security research, penetration testing, independent repair for security, and vulnerability disclosure and management. Drawing on the expertise of organizations that operate at the forefront of vulnerability discovery and disclosure, HPC has long advocated for policies that strengthen the security ecosystem while preserving the norms of responsible security research.

From this perspective, HPC strongly supports NIST's goal of maintaining a reliable, scalable, transparent, and broadly accessible vulnerability management ecosystem as advances in AI-enabled security research and frontier models dramatically increase the volume and complexity of vulnerability discovery and disclosure.

HPC's primary recommendation is that NIST should work with the broader vulnerability management community to better integrate NVD and the Common Vulnerabilities and Exposures (CVE) Program through a federated system for vulnerability information built on shared infrastructure and interoperable services. Today, CVE records are published and then separately ingested, reconciled, and enriched by the NVD. This separation creates duplication, delays, and additional operational complexity. As AI increases both software development and vulnerability discovery, these human-paced handoffs will become increasingly difficult to sustain.

Rather than publishing vulnerability information in one system and then separately ingesting, reconciling, enriching, and redistributing it through another, HPC recommends a unified CVE-NVD system built around a single authoritative vulnerability record. Core vulnerability information should be published promptly once minimum publication requirements are met, rather than held until enrichment is complete, and the authoritative record should then be progressively enriched as additional validated information becomes available. This approach would reduce duplicate processing, accelerate the propagation of updates, and shorten the path from disclosure to prioritization and remediation.

An integrated system should operate as an open ecosystem rather than a closed service. The system should build on existing machine-readable vulnerability formats and standards, including

CVE JSON, CSAF, VEX, and OSV where appropriate, with consistent use of established scoring and classification frameworks such as CVSS and CWE, rather than creating another competing vulnerability-data format. Stable and scalable public Application Programming Interfaces (APIs), bulk access, signed incremental updates, event-driven notifications, and complete version histories would allow CVE Numbering Authorities (CNAs), vendors, security researchers, and other trusted contributors to add attributable, machine-readable enrichment to the authoritative record. This enrichment information might include affected products and versions, severity, exploitability, mitigations, and remediation information.

The vulnerability ecosystem should rely on shared infrastructure and interoperable services that preserve distinct roles for NIST, CNAs, Authorized Data Publishers (ADPs), and other authorized contributors. NIST should continue to play an important role in validation and aggregation, while common infrastructure and processes support federated contribution and enrichment. The system should maintain one authoritative, versioned vulnerability record, publish core CVE information promptly, enrich that same record progressively, and provide common submission, validation, governance, and conflict-resolution mechanisms.

Integration should enable the vulnerability ecosystem to operate at greater speed and scale. The ecosystem must absorb both a near-term increase in vulnerability discovery and longer-term growth in the amount of software and vulnerabilities requiring management. Existing human-paced processes are already strained and will not scale to meet these demands. A unified system should therefore be designed around machine-readable data, AI-enabled automation, stable APIs, incremental updates, and near-real-time dissemination.

AI-enabled automation is particularly well suited to high-volume, repeatable tasks between disclosure and remediation. These include extracting and normalizing information from advisories and repositories, validating records and identifying duplicates or conflicts, and mapping vulnerabilities to products and versions. Human review should focus on particularly low-confidence, sensitive, or high-impact cases.

As AI accelerates both software development and vulnerability discovery, the vulnerability ecosystem will need to process substantially more information with greater speed and efficiency. Better integrating CVE and NVD around a single authoritative, continuously enriched vulnerability record would provide a more scalable foundation for that future. By reducing duplication, enabling federated enrichment, and supporting machine-readable and increasingly automated workflows, NIST and its partners across the vulnerability management ecosystem can strengthen the core vulnerability infrastructure on which researchers, vendors, security providers, and organizations depend.

Thank you for the opportunity to provide input to this Request for Information. If HPC can be of additional assistance, please contact Bri Law at BLaw@Venable.com.

Sincerely,

Hacking Policy Council