Hacking Healthcare - Weekly Blog

Aug 13, 2026

WHITE

View Alert

This week, Health-ISAC®'s Hacking Healthcare® highlights how a foundational resource in vulnerability management is attempting to adjust to the new realities of an AI world. Join us as we break down a newly published request for information from the National Institute of Standards and Technology (NIST) that seeks input on a wide array of potential changes to the National Vulnerability Database (NVD)

Welcome back to Hacking Healthcare®!

NIST Seeks Input on Revising the National Vulnerability Database in Response to AI

The rapid evolution of AI has reshaped the cyber threat landscape and led to warnings of an impending "vulnpocalypse" as threat actors' capabilities become augmented by AI tools.[i] In response to these concerns, the public and private sectors have begun efforts to harness AI for defensive purposes, including the use of frontier AI models to find vulnerabilities at speed and scale,[ii] and the development of vulnerability clearinghouses[iii] [iv] [v] [vi] to coordinate the resulting influx of data. The United States' NIST is among the latest to respond to this new reality by considering how the NVD could be revised.

What is the NVD?

The NVD is an important piece of the cybersecurity ecosystem. As they themselves explain, the NVD "provides the U.S. government repository of standards-based vulnerability management data," and "is a foundational resource for vulnerability management, software security, compliance automation, and cybersecurity risk analysis across the public and private sectors."[vii] The NVD helps to contextualize and enrich Common Vulnerabilities and Exposures (CVE) records, which are crucial to cyber defenders and tools.

Why is NIST seeking input?

NIST recognizes that AI is fundamentally changing the cyber threat landscape, and that the "inadequacies of traditional vulnerability management approaches, which center on periodic scanning, static prioritization, and often manual remediation, are increasingly apparent."[viii] For example, the significant growth in volume of identified vulnerabilities due to AI-enabled research, the complexity of new vulnerabilities, including the ability of AI to chain together multiple lower severity scored vulnerabilities, and resource and speed limitations of defenders all pose significant challenges that need to be met. To meet those challenges, NIST has decided that the NVD needs to evolve.

What is NIST seeking input on?

NIST describes the RFI as giving "the broader community an opportunity to identify forward-looking perspectives, practical recommendations, and innovative models to help shape the NVD moving forward."[ix] Topics it seeks feedback on include strategic planning, technical architecture decisions, standards and best practices development, data governance approaches, and community collaborations.

The RFI requests responses to questions across seven categories. Examples include:

- What other actions could NIST and others involved in the vulnerability management process take to improve vulnerability information dissemination?

- How can the NVD improve interoperability and integration with other vulnerability management ecosystem components (*e.g.*, vulnerability disclosure programs, vendor advisories, threat intelligence providers, asset management platforms, security tool vendors, remediation workflows) to enable more timely, accurate, actionable, and contextual vulnerability management?

Those interested in providing feedback must do so on or before October 13, 2026, at 11:59 p.m. Eastern Time.

Action & Analysis

Included with Health-ISAC Membership

[i] https://www.nbcnews.com/tech/security/anthropic-claude-mythos-ai-hackers-cybersecurity-vulnerabilities-rcna273673
[ii] https://www.anthropic.com/glasswing
[iii] https://www.whitehouse.gov/releases/2026/07/white-house-launches-gold-eagle-initiative-for-unprecedented-cybersecurity-vulnerability-coordination/
[iv] https://www.chainguard.dev/athena
[v] https://www.ibm.com/products/lightwell
[vi] https://akrites.org/
[vii] https://www.federalregister.gov/documents/2026/08/12/2026-16371/request-for-information-rfi-on-modernizing-the-national-vulnerability-database-in-the-age-of
[viii] https://www.federalregister.gov/documents/2026/08/12/2026-16371/request-for-information-rfi-on-modernizing-the-national-vulnerability-database-in-the-age-of
[ix] https://www.federalregister.gov/documents/2026/08/12/2026-16371/request-for-information-rfi-on-modernizing-the-national-vulnerability-database-in-the-age-of
[x] https://federalnewsnetwork.com/congress/2025/07/nist-to-get-funding-boost-under-house-bill/
[xi] https://cra.org/govaffairs/blog/2026/05/nist-nih-nasa-fy2027-pbr/
[xii] https://therecord.media/nist-to-limit-work-on-cve-entries-surge

<hr size=1 width="100%" align=center>

Alert Id	3376d991
Category	Hacking Healthcare
References	therecord federalnewsnetwork anthropic whitehouse federalregister chainguard nbcnews ibm cra akrites
Tags	National Vulnerability Database, Artificial Intelligence (AI), NVD, NIST, AI, CVE

Report Source(s)

Health-ISAC

Conferences, Webinars, and Summits
https://h-isac.org/events/

Hacking Healthcare
Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Councils efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Councils Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISACs annual Hobby Exercise and provides legal and regulatory updates for the Health-ISACs monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Threat Intelligence Portal
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments
Please email us at toc@h-isac.org

Please provide your feedback

Like Dislike

Download the App
Available on iOS, Android and Web

Download on the App Store Get it on Google Play

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**
Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to **toc@h-isac.org**