ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

700 K Street NW Suite 600
Washington, DC 20001

COMMENTS OF ITIF

to the

National Institute of Standards and Technology

Washington, D.C.

In the Matter of: Request for Information (RFI) on Modernizing the National Vulnerability Database in the Age of Artificial Intelligence	)	NIST-2026-0100

October 12, 2026

CONTENTS

Introduction and Summary 2
(1) Vulnerability Management Process 3
(2) Vulnerability Information Dissemination 5
(3) Risk Assessment and Prioritization 7
(4) Remediation Development, Deployment, and Monitoring 9
(5) Vulnerability Data and Standards 10
Conclusion 12

INTRODUCTION AND SUMMARY

The Information Technology and Innovation Foundation (ITIF) is pleased to submit these comments in response to the National Institute of Standards and Technology's (NIST) request for information on "Modernizing the National Vulnerability Database in the Age of Artificial Intelligence."[1] ITIF is a nonprofit, non-partisan public policy think tank based in Washington, D.C., committed to advancing pro-innovation, pro-technology, and pro-productivity policy agendas that strengthen economic growth and national competitiveness. As artificial intelligence (AI) reshapes the cybersecurity landscape, ITIF supports efforts to ensure federal vulnerability-management infrastructure remains reliable, scalable, and capable of supporting defenders operating at machine speed.

The rapid acceleration of AI-enabled vulnerability discovery has exposed structural weaknesses in the current vulnerability-management ecosystem. The National Vulnerability Database (NVD), built for human-speed discovery and manual enrichment, now faces increasing strain as AI-enabled disclosure volumes rise and exploitation timelines compress.[2] The Department of Commerce Inspector General recently found that the NVD backlog could more than double within 2026 alone, while frontier AI systems are already capable of identifying and chaining vulnerabilities far faster than existing validation and enrichment processes can absorb.[3] Without modernization, delays and data gaps in the NVD will spread into federal agencies, critical infrastructure operators, and the broader cybersecurity community that relies on timely, structured, and trustworthy vulnerability information.

---

[1] "Request for Information (RFI) on Modernizing the National Vulnerability Database in the Age of Artificial Intelligence, National Institute for Standards and Technology," August 8, 2026, https://www.federalregister.gov/documents/2026/08/12/2026-16371/request-for-information-rfi-on-modernizing-the-national-vulnerability-database-in-the-age-of.

[2] Anna Ribeiro, "NIST targets NVD modernization as AI transforms vulnerability discovery, risk assessment and remediation," *Industrial Cyber*, August 14, 2026, https://industrialcyber.co/nist/nist-targets-nvd-modernization-as-ai-transforms-vulnerability-discovery-risk-assessment-and-remediation/.

[3] Arthur L. Scott Jr., "Evaluation of NIST's Management of the National Vulnerability Database," United States Department of Commerce Office of the Inspector General, May 26, 2026, https://www.oig.doc.gov/wp-content/OIGPublications/OIG-26-020-I-SECURED.pdf.

ITIF strongly supports NIST's efforts to rebuild the NVD's technical architecture, strengthen interagency coordination, and adopt modernized workflows that incorporate automation while preserving essential human oversight. Modernization should prioritize machine-readable data, improved product-identification standards, clearer division of responsibilities between NIST and the Cybersecurity and Infrastructure Security Agency (CISA), and structured mechanisms for ingesting trusted information from vendors, researchers, and Common Vulnerabilities and Exposures Numbering Authorities.[4] It should also ensure transparency, auditability, and stakeholder engagement as core design principles. By addressing these challenges directly, NIST can restore confidence in the NVD, reduce duplication across the federal cybersecurity ecosystem, and ensure that vulnerability-management infrastructure remains effective in an era defined by AI-scale discovery and machine-speed exploitation.[5]

(1) VULNERABILITY MANAGEMENT PROCESS

A. Where in today's vulnerability management lifecycle (e.g., identifying, validating, disclosing, disseminating, prioritizing, remediating) are the biggest bottlenecks that could be improved with greater AI-enabled automation?

The greatest opportunity for AI-enabled automation within the NVD workflow lies in the validation, enrichment, and initial prioritization of newly disclosed vulnerabilities. The volume of disclosures has grown faster than NIST's ability to manually process and enrich them, creating backlogs that delay actionable information. In May 2026, the Department of Commerce Inspector General published a report.[6] that the NVD backlog could grow from 27,000 cases in 2025 to 60,000 by the end of 2026, underscoring that manual enrichment alone is no longer sufficient. Many of these vulnerability records already contain structured information from trusted vendors and researchers, meaning analysts spend valuable time reviewing information that automated systems could process more efficiently. Integrated AI-enabled tools could compare information across multiple sources, identify missing or inconsistent fields, detect duplicate submissions, and flag records that require additional review. Automation could handle routine, high-volume processing while reserving analysts for cases where human judgment adds the most value.

Additionally, the bottleneck is increasingly shifting from vulnerability discovery to validation and enrichment. AI systems can now identify and chain vulnerabilities at machine speed, while many downstream vulnerability management processes still rely on human review. Frontier AI companies, such as Anthropic and Google DeepMind, have demonstrated capabilities to use AI-powered vulnerability-detection systems to identify a growing number of vulnerabilities and potential exploit paths that organizations have to evaluate.[7] Recent

[4] Greg Otto, "Federal audit reveals NIST's NVD is plagued by poor planning and duplication," May 29, 2026, https://cyberscoop.com/nist-nvd-audit-mismanagement-duplication/.

[5] Greg Otto, "Federal audit reveals NIST's NVD is plagued by poor planning and duplication," May 29, 2026, https://cyberscoop.com/nist-nvd-audit-mismanagement-duplication/.

[6] Arthur L. Scott Jr., "Evaluation of NIST's Management of the National Vulnerability Database," United States Department of Commerce Office of the Inspector General, May 26, 2026, https://www.oig.doc.gov/wp-content/OIGPublications/OIG-26-020-I-SECURED.pdf.

[7] Corey Thomas et al., "Modernizing Global Vulnerability Standards," Rapid7, May 2026, https://www.rapid7.com/cdn/assets/blt9e44f1fe12d220b3/6a3ba488267c429f40ff951a/Modernizing_Global_Vulnerability_Standards.pdf.

analyses highlights that exploitation often occurs with 24 hours of disclosure, making timely validation and enrichment increasingly important for defenders.[8]

B. Which tasks are most appropriate for AI-enabled automation? Which tasks should require human review? For tasks requiring human review, what information is needed, and how can reviews be arranged to both minimize time spent and avoid over-reliance on AI?

AI tools are best suited for tasks involving large volumes of information, recurring patterns, or well-defined objectives, including many tasks involving unstructured information and non-routine decisions. For the NVD, helpful tasks for AI include identifying missing fields, detecting duplicate records, comparing vulnerability information across trusted sources, and flagging records for additional review. Automating these processes could enable NIST to process routine vulnerabilities more quickly while establishing a consistent basis for determining which cases require additional attention. NIST should prioritize analyst review of instances when information is disputed or contradictory, when a vulnerability could have significant consequences, or when structured data cannot reliably capture technical context.

Analysts should also receive the key data underlying each automated assessment, such as the original source information, any inconsistencies the system identified, and a concise explanation of why the record was escalated, so they can independently verify the basis for the recommendation. This would allow reviewers to evaluate the underlying evidence rather than simply accept an AI-generated conclusion.

Similarly, automated reachability analysis could indicate whether real-world deployments are using vulnerable code, while analysts could validate cases where reachability depends on complex configurations or call paths. This approach would reduce the amount of information analysts must create manually while preserving essential oversight over consequential decisions and reporting.

D. What other actions could NIST and others involved in the vulnerability management process take to improve vulnerability management processes?

NIST and the CISA should establish a clearer division of responsibilities so that the two agencies do not duplicate enrichment and analysis tasks. CISA's operational focus on actively exploited vulnerabilities complements NIST's role in maintaining the broader vulnerability database and supporting vulnerability-management standards. Formalizing these responsibilities could allow each agency to concentrate limited resources where they provide the most value.[9]

[8] "What the NVD 'Slowdown' Means For You: How to Stay Ahead in Vulnerability Management," FlashPoint, April 1, 2026, https://flashpoint.io/blog/nvd-slowdown-stay-ahead-vulnerability-management/; Patrick Garrity, "State of Exploitation – A look into The 1H-2025 Vulnerability Exploitation & Threat Activity," VulnCheck, July 30, 2025, https://www.vulncheck.com/blog/state-of-exploitation-1h-2025.

[9] Jaikumar Jijayan, "CISA's 'vulnerichment' aims to fix the NVD," *Reversing Labs*, May 15, 2024, https://www.reversinglabs.com/blog/cisas-new-vulnrichment-program-attempts-to-address-nvd-slowdown.

NIST should also modernize processes for managing vulnerability and product information. Replacing email-based Common Platform Enumeration (CPE) submissions with a structured portal could make it easier to validate and incorporate product information while reducing manual administrative work.[10]

(2) VULNERABILITY INFORMATION DISSEMINATION

A. What capabilities, products, and processes, AI or otherwise, are needed to improve the responsible and timely dissemination of vulnerability information to technology developers and the broader community of affected stakeholders?

Improving dissemination requires NIST to make vulnerability information timelier, more consistently structured for automated use, machine-readable, and interoperable. Organizations increasingly consume vulnerability data through automated systems, so delays or inconsistencies in NVD records can spread into downstream tools and slow the identification of affected systems.[11] NIST should prioritize systems that allow validated information from trusted sources to enter the NVD with minimal manual processing. Greater automation could allow organizations to receive actionable information sooner while reducing the burden on NIST analysts.

Organizations should also have greater visibility into the status and completeness of vulnerability records. The NVD should evolve from simply indicating that a vulnerability exists to providing more context about its practical risk, including exploit-chain involvement, reachability, and AI-demonstrated exploitability when independently verified. Structured chain-risk metadata could indicate whether a vulnerability is part of a known exploit chain and the severity of the resulting exploit.[12]

NIST should also create and publish machine-readable completeness indicators so downstream systems can distinguish between fully enriched records and those still under review. These capabilities would help organizations prioritize vulnerabilities based on their practical risk rather than relying on basic severity scores.

B. What existing standards and technical guidelines are most helpful for disseminating vulnerability information? What gaps in standards and guidelines exist? How should addressing those gaps be prioritized?

Existing standards such as Common Vulnerabilities and Exposures (CVE) and Common Platform Enumeration (CPE) provide an important foundation for vulnerability information sharing. Their usefulness, however, depends on the quality and consistency of the information associated with each record. NIST should therefore prioritize improving the implementation and interoperability of existing standards before creating entirely new ones. CPE's modernization should be a particular priority because inaccurate or

---

[10] "Official Common Platform Enumeration (CPE) Dictionary," National Institute for Standards and Technology, https://nvd.nist.gov/products/cpe.

[11] Ross Kelly, "'The economics of vulnerability discovery have changed': NIST wants to modernize the National Vulnerability Database amid AI advances – cyber experts say it needs to be redesigned with machine-speed in mind," *IT Pro*, August 20, 2026, https://www.itpro.com/security/nist-national-vulnerability-database-modernization-machine-speed-consumption.

[12]"What the NVD 'Slowdown' Means For You: How to Stay Ahead in Vulnerability Management," FlashPoint, April 1, 2026, https://flashpoint.io/blog/nvd-slowdown-stay-ahead-vulnerability-management/.

incomplete product information can prevent organizations from identifying affected assets.[13] A secure, structured submission portal with automated validation could replace the current email-based process, reducing delays and improving data quality.

NIST should also integrate existing machine-readable formats—such as the Common Security Advisory Framework, which vendors use to publish structured security advisories, and the Vulnerability Exploitability eXchange (VEX), which clarifies whether a vulnerability affects a product—more directly into NVD ingestion pipelines.[14] These standards can provide structured advisory and exploitability information without requiring NIST analysts to recreate data that already exists elsewhere. Additional standards or metadata should also support emerging needs such as exploit-chain risk and reachability, allowing vulnerability information to become more useful for contextual prioritization.[15]

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

NIST should strengthen the mechanisms through which information moves between organizations that discover, analyze, and consume vulnerability information. Vendors, researchers, CVE Numbering Authorities, and other organizations often possess information that can improve a vulnerability record, but requiring NIST analysts to manually reconstruct that information introduces unnecessary delays.[16] NIST should establish standardized mechanisms for ingesting and validating structured information from trusted sources and publish performance metrics, such as processing timelines and backlog levels, so stakeholders can assess whether dissemination is improving.

NIST should also move toward a federated enrichment model in which CVE Numbering Authorities, vendors, and qualified data publishers contribute structured information, while NIST serves as the trusted aggregation and normalization layer. This approach could distribute routine enrichment across organizations that already possess relevant information while allowing NIST to focus on validation, consistency, and quality control.[17] NIST should also publish real-time enrichment-completeness indicators so organizations can determine whether a record includes comprehensive product information, validated exploitability data, or

[13] "Official Common Platform Enumeration (CPE) Dictionary," National Institute for Standards and Technology, https://nvd.nist.gov/products/cpe.

[14] "Toward greater transparency: Publishing machine-readable CSAF files," Microsoft, November 12, 2024, https://www.microsoft.com/en-us/msrc/blog/2024/11/toward-greater-transparency-publishing-machine-readable-csaf-files; Lisa Olson, "Toward greater transparency: Introducing machine-readable Vulnerability Exploitability Xchange (VEX) for Azure Linux and beyond," Microsoft, October 22, 2025, https://www.microsoft.com/en-us/msrc/blog/2025/10/toward-greater-transparency-machine-readable-vulnerability-exploitability-xchange-for-azure-linux.

[15] Jonathan Stross, "Comparison of Vulnerability Management Framework: CISA, NIST, SANS," Pathlock, June 2, 2025, https://pathlock.com/learn/comparison-of-vulnerability-management-frameworks/.

[16] Zeljka Zorz, "How NIST fumbled management of the National Vulnerability Database," *Helpnet Security*, June 1, 2026, https://www.helpnetsecurity.com/2026/06/01/nist-nvd-management-problems/.

[17] Ionut Arghire, "NIST Prioritizes NVD Enrichment for CVEs in CISA KEV, Critical Software," *Security Week*, April 16, 2026, https://www.securityweek.com/nist-prioritizes-nvd-enrichment-for-cves-in-cisa-kev-critical-software/.

pending metadata. Together, these changes could make vulnerability information timelier and more useful without requiring NIST to perform every enrichment task internally.

(3) RISK ASSESSMENT AND PRIORITIZATION

A. How can the use of AI or other automated mechanisms improve contextual risk prioritization? What data sources and information should be considered by NIST to inform prioritization decisions?

AI tools, such as Amazon's agentic RuleForge system, which generates and validates vulnerability-detection rules far faster than manual methods, can help NIST move beyond treating severity as a sufficient proxy for risk.[18] A vulnerability's practical importance depends on factors such as product prevalence, evidence of exploitation, exploit-chain involvement, and the completeness of available information. Automated systems can combine these signals across large numbers of vulnerabilities much faster than human analysts, allowing NIST to identify cases that warrant greater attention. NIST should use AI tools to surface and contextualize these signals, however, as today's automated systems can at times misinterpret ambiguous evidence or over-weight incomplete signals, human review may at times be necessary to ensure that any escalation are grounded in accurate, validated risk.[19]

Once NIST establishes independent verification standards, AI-demonstrated exploitability could also become a useful triage signal. If an AI system produces a working exploit for a vulnerability before analysts observe an exploit in the wild, that finding provides validated evidence of practical exploitability, giving analysts an opportunity to review and prioritize the vulnerability before attackers use it in an attack. This signal would complement existing threat intelligence, since exploits may already be circulating privately or on criminal marketplaces before attackers deploy them.[20] NIST should also incorporate chain-risk metadata into prioritization workflows so vulnerabilities that contribute to high-impact exploit chains receive appropriate urgency. Reachability information could further distinguish between theoretical severity and vulnerabilities that affect code used in real-world environments. Combining these signals could give defenders a more accurate picture of which vulnerabilities require immediate attention.

B. How might transparency and auditability in AI-driven prioritization decisions be enhanced?

AI-driven prioritization should be explainable, source-traceable, and auditable. Automated systems should provide the evidence used to generate each prioritization signal, identify the sources of that evidence, indicate the system's confidence, and explain why the system escalated a vulnerability. This information would allow

[18] C. J. Moses, "How Amazon uses agentic AI for vulnerability detection at global scale," *Amazon Science*, April 8, 2026, https://www.amazon.science/blog/how-amazon-uses-agentic-ai-for-vulnerability-detection-at-global-scale.

[19] Jonathan Stross, "Comparison of Vulnerability Management Framework: CISA, NIST, SANS," Pathlock, June 2, 2025, https://pathlock.com/learn/comparison-of-vulnerability-management-frameworks/; Junic Kim and Haeyong Shin, "Stage-Aware Governance of Large Language Models: Managing Uncertainty and Human Oversight in AI-Assisted Literature Review Systems, Konkuk University, December 2025, https://www.mdpi.com/2079-8954/14/2/153.

[20] "Can NVD Modernization Keep Pace with AI?," *SOCRadar*, August 18, 2026, https://socradar.io/blog/can-nvd-modernization-keep-pace-with-ai/.

analysts to evaluate the basis for an automated recommendation rather than treating the system's output as a final determination.[21]

NIST should also require automated systems to maintain a structured audit trail showing how the system reached each prioritization decision. The record should include relevant chain-risk indicators, reachability signals, exploitation evidence, and changes to the underlying information over time. Analysts should be able to reconstruct and review the decision path to validate or challenge an automated assessment. These safeguards could make AI-assisted prioritization more transparent while preserving meaningful human oversight.

D. 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?

The NVD should function less as an isolated database and more as an interoperable information layer within the broader vulnerability management ecosystem. Vulnerability information originates from vendors, researchers, and threat intelligence providers, while organizations consume that information through asset-management and security platforms. NIST should therefore prioritize standardized, machine-readable data exchanges that allow information to move efficiently between these systems.[22]

Additionally, the NVD should integrate relevant operational information, including CISA's Known Exploited Vulnerabilities catalog, exploit-chain data, and reachability information from vulnerability discovery programs.[23] Improved CPE data is also essential for mapping vulnerabilities to affected assets; without reliable product identifiers, automated prioritization and remediation workflows cannot operate effectively.[24] Better interoperability would allow organizations to combine vulnerability information with their own threat data, giving them a clearer basis for deciding which vulnerabilities to address first.

E. What other actions could NIST and others involved in the vulnerability management process take to improve risk assessment and prioritization?

NIST should work more closely with CISA and other organizations that maintain operational information about vulnerabilities. A clearer division of responsibilities and structured information-sharing mechanisms

---

[21] Ross Kelly, "'The economics of vulnerability discovery have changed': NIST wants to modernize the National Vulnerability Database amid AI advances – cyber experts say it needs to be redesigned with machine-speed in mind," *IT Pro*, August 20, 2026, https://www.itpro.com/security/nist-national-vulnerability-database-modernization-machine-speed-consumption.

[22] "What the NVD 'Slowdown' Means For You: How to Stay Ahead in Vulnerability Management," FlashPoint, April 1, 2026, https://flashpoint.io/blog/nvd-slowdown-stay-ahead-vulnerability-management/.

[23] "Known Exploited Vulnerabilities Catalog (KEV)," ARMO, https://www.armosec.io/glossary/known-exploited-vulnerabilities-catalog-kev/.

[24] "Official Common Platform Enumeration (CPE) Dictionary," National Institute for Standards and Technology, https://nvd.nist.gov/products/cpe.

would allow NIST to incorporate operational context without duplicating CISA's analysis.[25] NIST's recent shift move toward risk-based triage also demonstrates the need to redesign enrichment and prioritization workflows to handle growing volumes of vulnerability information. Modernization should therefore focus on approaches—such as structured data-exchange standards and risk-based triage models—that can process AI-scale discovery while directing limited analyst resources and time toward the vulnerabilities where human judgment is key.[26]

NIST should also coordinate internationally to ensure that vulnerability-management standards remain interoperable across jurisdictions. Engagement with organizations such as the European Union Agency for Cybersecurity, Five Eyes partners, and the United States-European Union Trade and Technology Council could help align approaches to vulnerability identifiers, product information, and risk assessment.[27] Greater interoperability could reduce duplication for organizations operating across multiple countries and make vulnerability information more useful throughout the global cybersecurity ecosystem.

(4) REMEDIATION DEVELOPMENT, DEPLOYMENT, AND MONITORING

A. What new mechanisms, standards, and procedures may be necessary for automated vulnerability remediation? What role, if any, should AI systems have in automated vulnerability remediation?

Automated remediation depends on accurate, timely, and machine-readable vulnerability and product information. AI systems could eventually assist with tasks, such as proposing patches or recommending configuration changes, but these capabilities should operate within standards that ensure automated fixes are safe and effective. NIST should therefore explore standards for machine-readable remediation instructions, configuration-specific reachability information, and automated validation of vendor-provided patches. AI-generated remediation, as with any proposed remediation, should also undergo independent verification before deployment because new code can introduce subtle or unexpected errors, such as omitting a necessary validation check or generating a patch that compiles but breaks dependencies. Independent review could catch these errors before deployment, confirming that the fix addresses the original vulnerability without introducing new risks.[28]

NIST should also work with vendors to standardize machine-readable patch and remediation metadata so security tools can identify appropriate fixes and incorporate them into existing workflows. This would allow organizations to automate routine remediation while maintaining human oversight for changes that could

---

[25] Jaikumar Jijayan, "CISA's 'vulnerichment' aims to fix the NVD," *Reversing Labs*, May 15, 2024, https://www.reversinglabs.com/blog/cisas-new-vulnrichment-program-attempts-to-address-nvd-slowdown.

[26] "NVD Enrichment Triage: Enterprise Vulnerability Programs Must Adapt," CSA, April 19, 2026, https://labs.cloudsecurityalliance.org/research/csa-research-note-nist-nvd-enrichment-policy-change-20260419/.

[27] Suzanne Smalley, "Inspector general finds NIST mistakes have made vulnerability database ineffective," *The Record*, June 1, 2026, https://therecord.media/nist-mistakes-vulnerability-database-inspector-general.

[28] "Can NVD Modernization Keep Pace with AI?," SOCRadar, August 18, 2026, https://socradar.io/blog/can-nvd-modernization-keep-pace-with-ai/; Asaf Saar, "Why AI Can't Verify Its Own Code and What That Means for Enterprise AppSec," Mend.io, June 16, 2026, https://www.mend.io/blog/ai-generated-code-security-independent-verification/; Rodrigo Pato Nogueira et al., "Unreliable in Practice? A Comprehensive Study of Errors in LLM-Generated Code," ARXIV, August 2026, https://arxiv.org/html/2608.00661v1.

affect critical systems or create new security risks. Establishing common formats and validation requirements would also make it easier for organizations to determine whether automated remediation is appropriate for their specific environment.[29]

F. What other actions could NIST and others involved in the vulnerability management process take to improve vulnerability remediation development, deployment, and monitoring?

NIST should coordinate with CISA, CVE Numbering Authorities, and major vendors to ensure remediation guidance remains consistent across vendor advisories, Known Exploited Vulnerabilities entries, and NVD records.[30] NIST should also publish remediation-related data-quality metrics, including the completeness of affected-product lists, timeliness of updates, and accuracy of configuration-specific guidance. These measures would help identify where gaps in vulnerability information could prevent organizations from taking effective action.

The NVD should also provide machine-readable indicators showing whether a vulnerability has been fully remediated, partially mitigated, or remains unaddressed when that information is available. This would allow security and asset-management platforms to incorporate remediation status into automated workflows and give organizations a clearer picture of outstanding risk.[31] Connecting remediation information more closely with vulnerability records could help move the NVD from simply documenting vulnerabilities toward supporting the full vulnerability-management process.

(5) VULNERABILITY DATA AND STANDARDS

A. What changes are needed in organizational structures, processes, procedures, standards, and specifications to improve the quality of vulnerability data?

Improving vulnerability data quality requires addressing both the information entering the NVD and the processes used to validate it. Automated validation should identify missing fields, inconsistencies, and duplicate records, while analysts resolve cases where automated checks identify uncertainty or conflicting information. NIST should also modernize how product information enters the system by replacing manual CPE submissions with a structured portal, which could automatically validate product names, check for duplicates, enforce formatting rules, and streamline updates from vendors.[32] These changes would reduce routine processing burdens while giving analysts more time to address complex data-quality issues.

Disclosure and enrichment workflows should also account for the growing use of AI systems in vulnerability discovery. As these systems become more capable at identifying large volumes of vulnerabilities in short periods, processes designed around human-speed discovery will no longer provide enough time for defenders

---

[29] Zeljka Zorz, "How NIST fumbled management of the National Vulnerability Database, Helpnet Security, June 1, 2026, https://www.helpnetsecurity.com/2026/06/01/nist-nvd-management-problems/.

[30] "Known Exploited Vulnerabilities Catalog (KEV)," ARMO, https://www.armosec.io/glossary/known-exploited-vulnerabilities-catalog-kev/.

[31] "What the NVD 'Slowdown' Means For You: How to Stay Ahead in Vulnerability Management," FlashPoint, April 1, 2026, https://flashpoint.io/blog/nvd-slowdown-stay-ahead-vulnerability-management/.

[32] "Official Common Platform Enumeration (CPE) Dictionary," National Institute for Standards and Technology, https://nvd.nist.gov/products/cpe.

to validate and act on findings.[33] NIST should work with AI frontier laboratories to establish standardized information packages for AI-generated vulnerability findings, including discovery methodology, known failure modes, and metadata describing optimal deployment conditions.[34] This information could enable NIST and other stakeholders to evaluate AI-generated findings quickly, determining which signals warrant additional verification and analysis.

B. Are existing standards, context, and specifications for vulnerability data, including vulnerability identifiers, product naming schemes, and severity scoring systems, sufficient for improving actionable prioritization of vulnerabilities in the AI era? If so, please describe.

Existing standards provide an important foundation for the NVD, but NIST should focus on making them more reliable, interoperable, and useful to automated systems. T he Common Vulnerability Scoring System remains useful for communicating baseline severity, but it does not capture several factors increasingly important to AI-era prioritization, such as whether AI systems have demonstrated that a vulnerability can be exploited in practice. Rather than modifying severity scores, NIST should consider adding structured metadata to CVE and NVD records to capture these factors.[35] This addition could allow organizations to distinguish between vulnerabilities that appear severe in theory and those that pose an immediate practical threat.

Product naming should also require continued modernization to support automated asset mapping, ensuring that tools can reliably match vulnerabilities to the correct software. Inconsistent or incomplete CPE information can prevent organizations from accurately determining which systems are affected, limiting the effectiveness of automated prioritization and remediation.[36] Improving product identifiers and interoperability should therefore remain a priority alongside efforts to expand contextual risk information.

F. What other actions could NIST and others involved in the vulnerability management process take to improve vulnerability data and standards?

NIST should create structured opportunities for stakeholders to identify weaknesses in vulnerability data and standards. A permanent advisory group could bring together industry, academia, researchers, and other approved users of the NVD to evaluate whether proposed changes improve usability, transparency, and

[33] "What the NVD 'Slowdown' Means For You: How to Stay Ahead in Vulnerability Management," FlashPoint, April 1, 2026, https://flashpoint.io/blog/nvd-slowdown-stay-ahead-vulnerability-management/.

[34] Corey Thomas et al., "Modernizing Global Vulnerability Standards," Rapid7, May 2026, https://www.rapid7.com/cdn/assets/blt9e44f1fe12d220b3/6a3ba488267c429f40ff951a/Modernizing_Global_Vulnerability_Standards.pdf.

[35] Jonathan Stross, "Comparison of Vulnerability Management Framework: CISA, NIST, SANS," Pathlock, June 2, 2025, https://pathlock.com/learn/comparison-of-vulnerability-management-frameworks/; Dan DeCloss, "Why CVSS Scores Don't Tell the Real Story of Risk," *The Hacker News*, March 9, 2026, https://thehackernews.com/expert-insights/2026/03/why-cvss-scores-dont-tell-real-story-of.html.

[36] "Official Common Platform Enumeration (CPE) Dictionary," National Institute for Standards and Technology, https://nvd.nist.gov/products/cpe; Yuning Jiang et al., "VulCPE: Context-Aware Cybersecurity Vulnerability Retrieval and Management," May 20, 2025, https://arxiv.org/pdf/2505.13895.

machine-readability.[37] A formal feedback mechanism would also give NIST a consistent way to identify recurring problems and assess whether changes are addressing the needs of the organizations relying on the NVD.

CONCLUSION

Overall, modernizing the National Vulnerability Database requires more than incremental improvements, it demands a structural redesign that reflects the realities of AI-driven vulnerability discovery and machine-speed exploitation. NIST should modernize the NVD by expanding automation, improving coordination with CISA, and adopting more reliable product-identification and data-ingestion systems that support machine-speed defense. These reforms could ensure that vulnerability information is timely, trustworthy, and actionable for both government and industry. By rebuilding the NVD around transparency, interoperability, and machine-readable data, NIST can restore confidence in the nation's vulnerability-management infrastructure and position the United States to defend effectively in a cybersecurity environment increasingly shaped by artificial intelligence.

Thank you for your consideration.

David Kertai
Research Assistant
Information Technology and Innovation Foundation

[37] "CISA Announces New Town Halls to Engage with Stakeholders on Cyber Incident Reporting for Critical Infrastructure," Cybersecurity and Infrastructure Security Agency, February 13, 2026, https://www.cisa.gov/news-events/news/cisa-announces-new-town-halls-engage-stakeholders-cyber-incident-reporting-critical-infrastructure; Suzanne Smalley, "Inspector general finds NIST mistakes have made vulnerability database ineffective," *The Record*, June 1, 2026, https://therecord.media/nist-mistakes-vulnerability-database-inspector-general.