ode: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket Number: 260805-0401]

XRIN: 0693-XC139

Request for Information (RFI) on Modernizing the National Vulnerability Database in the Age of Artificial Intelligence

AGENCY: Information Technology Laboratory (ITL), National Institute of Standards and Technology (NIST), U.S. Department of Commerce.

ACTION: Notice; Request for Information (RFI).

SUMMARY: The National Institute of Standards and Technology (NIST) established and operates the National Vulnerability Database (NVD), which provides the U.S. government repository of standards-based vulnerability management data. NIST seeks stakeholder input on opportunities, challenges, and priorities for modernizing the NVD in an evolving cybersecurity landscape increasingly shaped by artificial intelligence (AI) and machine-consumable security data. NIST's goal is to improve the NVD's scalability, automation, interoperability, transparency, and utility.

DATES: Comments in response to this notice must be received on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], at 11:59 p.m. Eastern Time. Submissions received after that date may not be considered.

ADDRESSES: Comments must be submitted electronically via the Federal e-Rulemaking Portal.

1. Go to www.regulations.gov and enter NIST-2026-0100 in the search field;

2. Click the "Comment Now!" icon, complete the required fields, including the relevant document number and title in the subject field; and

3. Enter or attach your comments.

Additional information on the use of regulations.gov, including instructions for accessing agency documents, submitting comments, and viewing the docket is available at: www.regulations.gov/faq. If you require an accommodation or cannot otherwise submit your comments via regulations.gov, please contact NIST using the information in the FOR FURTHER INFORMATION CONTACT section below.

NIST will not accept comments for this notice by postal mail, fax, or email. To ensure that NIST does not receive duplicate copies, please submit your comments only once. Comments containing references, studies, research, and other empirical data that are not widely published should include copies of the referenced materials.

All relevant comments received by the deadline will be posted at: https://www.regulations.gov under docket number NIST-2026-0100 without change or redaction, so commenters should not include information they do not wish to be posted publicly (e.g., personal or confidential business information).

FOR FURTHER INFORMATION CONTACT: For questions about this RFI contact: Cristina Ritfeld, NVD-RFI@nist.gov. Direct media inquiries to NIST's Communications and Outreach Office at (301) 975-2762. Users of telecommunication devices for the deaf, or a text telephone may call the Federal Relay Service toll free at 1-800-877-8339. NIST will make the RFI available in alternate formats, such as Braille or large print, upon request by persons with disabilities.

SUPPLEMENTARY INFORMATION: The National Vulnerability Database (NVD), established and operated by NIST, provides the U.S. government repository of standards-based vulnerability management data. The NVD is a foundational resource for vulnerability management, software security, compliance automation, and cybersecurity risk analysis across the public and private sectors. It provides standardized vulnerability enrichment and associated metadata consumed by a broad ecosystem of security tools and operational workflows. It is a part of the broader vulnerability management ecosystem that encompasses processes, standards, and tools involved in one or more phases of the vulnerability lifecycle of identifying, validating, disclosing, disseminating, prioritizing, and remediating software and system vulnerabilities.

Today, the NVD ingests Common Vulnerabilities and Exposures (CVE) records[1] within approximately an hour of publication using automated processes. NVD analysts then enrich CVE records with additional information and analysis such as severity scores and affected product versions. Users and security tools can access the enriched CVE records through the NVD's web interface or through automated mechanisms.

Today's vulnerability management ecosystem is rapidly evolving and is characterized by AI-enabled cyber tools and accelerated technology delivery cycles. Malicious actors may seek to leverage AI systems to discover and exploit vulnerabilities at scale and to support post-exploitation activities. The inadequacies of traditional vulnerability management approaches, which center on periodic scanning, static prioritization, and manual remediation, are increasingly apparent. Several trends present both challenges and opportunities for modernization, including the growth in the volume and complexity of disclosed vulnerabilities; a range in the quality of data; increased reliance on automation and machine-readable security data; the expansion of technology security risk management practices; the emergence of AI-assisted vulnerability discovery, triage, exploitation, and remediation; demand for near real-time vulnerability enrichment; and resource constraints associated with scaling vulnerability analysis and enrichment activities.

The advancement of AI presents an opportunity to transform the vulnerability management ecosystem. This requires input from across the community to ensure this ecosystem is effective, scalable, and resilient in the face of emerging threats. NIST plays a key role in this ecosystem, which also relies on other organizations and individuals, including those who identify, evaluate, provide, and implement solutions to manage cybersecurity risks. NIST intends to support a future-ready vulnerability management ecosystem that is continuous, contextual, and automated, while enabling cybersecurity practices to respond appropriately to real-world threats and business priorities.

NIST is using this RFI to give the broader community an opportunity to identify forward-looking perspectives, practical recommendations, and innovative models to help shape the NVD moving forward. Responses are intended to inform future strategic planning, technical architecture decisions, standards and best practices development, data governance approaches, and community collaborations related to the continued evolution of the NVD.

[1] https://www.cve.org/Downloads

NIST seeks stakeholder perspectives on how the NVD can grow to better support cybersecurity outcomes while maintaining trust, transparency, accuracy, and broad accessibility.

Request for Information:

This RFI provides the broader community an opportunity to identify forward-looking perspectives, practical recommendations, and innovative models to help shape the NVD. Respondents are encouraged to address any or all of the following questions.

(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?

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?

c. What are the novel governance and risk management considerations that should be taken into account in modernizing the vulnerability management ecosystem?

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

(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?

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?

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

(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?

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

c. What data and system context is needed by organizations to prioritize vulnerabilities accurately in production environments?

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?

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

(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?

b. What organizational structures, policies, processes, and frameworks are needed for organizations and open-source projects to manage AI-generated remediations?

c. What controls and safeguards are needed to prevent erroneous AI-generated remediations?

d. What are the biggest barriers to stakeholders (e.g., users, developers, organizations) remediating vulnerabilities after they receive prompt and comprehensive vulnerability information?

e. What process and organizational dependencies (e.g., discovery and asset inventory) are prerequisites for organizations to more fully operationalize automated vulnerability remediation?

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

(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?

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.

c. What gaps are there in existing standards and specifications?

d. What information is needed for organizations to efficiently and effectively manage the increasing number of identified vulnerabilities, including vulnerability prioritization and product identification?

e. What changes are needed to improve machine-readable vulnerability data (e.g., data in the NVD) to improve vulnerability prioritization and contextualization?

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

(6) Development Processes

a. How can organizations effectively integrate AI-enabled tools into technology development processes to proactively identify, reduce, and remediate security vulnerabilities, and to enhance overall vulnerability management practices throughout the system lifecycle? What changes, if any, are needed to processes, procedures, standards, and specifications to enable this integration.

(7) Vision for the NVD

a. What has been the value of the NVD to organizations? To the extent practicable, please describe how organizations may use the NVD and what activities or decisions the NVD informs.

b. What capabilities and services can be integrated into the NVD to increase its impact over the next five years?

c. What emerging cybersecurity trends relevant to the vulnerability management should the NVD anticipate over the next five years?

d. What capabilities and services will enhance the NVD's utility for vulnerability analysts, technology developers, researchers, and policymakers?

e. What metrics should be considered to track and evaluate the success of the NVD and any modernization efforts?

Authority: 15 U.S.C. §§ 272(b),(c) and 278g-3.

Alicia Chambers,
NIST Executive Secretariat.
[FR Doc. 2026-16371 Filed: 8/11/2026 8:45 am; Publication Date: 8/12/2026]