



October 13, 2026

National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

VIA ELECTRONIC SUBMISSION

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

HackerOne Inc. (HackerOne) 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) or super intelligence (SI).¹ HackerOne appreciates NIST's continued work to strengthen the NVD and welcomes the opportunity to provide recommendations.

HackerOne is a global leader in Continuous Threat Exposure Management (CTEM) and the only solution provider that pairs the simultaneous trust of the Fortune 500 and the world's largest community of security researchers to secure the AI-native enterprise. The H1 Platform unites agentic AI solutions with security researchers' ingenuity to continuously discover, validate, prioritize, and remediate exposures across code, cloud, and AI systems. Through solutions such as agentic and human offensive security testing, AI red teaming, code security, validation, and remediation, HackerOne delivers measurable, continuous reduction of cyber risk for enterprises. Industry leaders, including Anthropic, Crypto.com, General Motors, Goldman Sachs, Lufthansa, Uber, UK Ministry of Defence, and the U.S. Department of Defense, trust HackerOne to safeguard their digital ecosystems.

The NVD is a foundational resource for vulnerability management across the public and private sectors. As the volume of reported vulnerabilities continues to grow and AI changes how vulnerabilities are discovered, analyzed, and potentially exploited, modernizing the NVD is essential to ensuring that vulnerability information remains timely, accurate, and useful. HackerOne supports NIST's efforts to explore how AI and automation can help the NVD operate at greater scale while preserving the human expertise, transparency, and quality controls necessary to maintain trust in the data. Drawing on our experience, we offer recommendations in four areas of the RFI: the vulnerability management process, vulnerability information dissemination, risk assessment and prioritization, and the long-term vision for the NVD. Throughout, our central message is that AI should be used to scale proven processes and focus human expertise, not to replace them.

¹ National Institute of Standards and Technology, *Request for Information (RFI) on Modernizing the National Vulnerability Database in the Age of Artificial Intelligence*, 91 Fed. Reg. 52042 (Aug. 12, 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->

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?

Today, the biggest bottleneck in the vulnerability management lifecycle is validation and remediation. AI is rapidly increasing the speed and scale at which vulnerabilities can be discovered, and this trend will accelerate as frontier models become more capable of identifying vulnerabilities with greater speed. As discovery scales, so too will the number of findings that organizations must process. Each of those findings still needs to be evaluated to determine whether it is legitimate, reproducible, novel, and presents a meaningful security risk. Finding more vulnerabilities only improves security if organizations can efficiently validate, prioritize, and ultimately remediate them.

Validation. A large volume of unvalidated findings can consume limited security resources, slow the review of legitimate vulnerabilities, and make it harder to spot the greatest risks. HackerOne has seen this firsthand in H1 Platform data: vulnerability submissions rose 45% year over year as of June 2026, while only about 21% of findings were confirmed to be exploitable.

Remediation. Fixing is where risk is actually reduced, and it is often the slowest step. HackerOne data shows that the backlog of critical vulnerabilities has grown 29 times, even as the average time to fix critical findings (mean time to remediate) has improved 53%. Validated findings still wait weeks to be fixed, and medium and low severity findings often sit indefinitely because teams lack the time to make the case for fixing them.

The answer is not to replace existing processes or the security professionals who run them. It is to equip those processes to handle higher volume, so security teams spend less time sorting findings and more time where they are needed most.

(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 is best suited to tasks that involve processing large volumes of information, performing repeatable work, and identifying patterns that can help security teams determine where to focus their attention. For example, AI can assist with initial triage, identify duplicate or previously known vulnerabilities, correlate information across reports and other data sources, and surface findings that warrant closer review.

HackerOne is already applying this model through [HackerOne AI \(Hai\)](#), its agentic AI orchestration system. Hai coordinates specialized AI agents across vulnerability discovery, validation, prioritization, and remediation workflows. This allows AI to automate repeatable tasks and help move information through different stages of the vulnerability lifecycle, while escalating findings that require additional technical expertise or judgment. [H1 Agentic Pentesting](#) follows a similar approach, pairing autonomous AI agents that can perform tasks such as reconnaissance, testing, exploitation, and validation at scale with human security experts who review and verify findings.

Human guidance and input remains essential. Security professionals bring technical expertise and context that AI cannot provide on its own, particularly when a finding is novel, ambiguous, or depends on the specific environment in which a vulnerability exists. Human experts can direct how AI is applied, judge real-world exploitability and impact, recognize unexpected behavior or attack paths, and flag when an automated assessment does not fully capture the risk a vulnerability presents.

NIST's goal should therefore be to make human review more focused and efficient when it is required. AI can organize the underlying technical evidence, relevant context, and related vulnerability information before a finding reaches a reviewer, reducing the time spent gathering and sorting information. But human reviewers should still have access to the underlying evidence and sufficient context to independently assess a finding, challenge an AI-generated conclusion, and determine when additional review may be needed. Reviewer feedback and guidance will also help improve the AI's future assessments and ensure alignment with overall goals.

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?

NIST should build on the vulnerability disclosure processes that already work rather than create separate processes for AI-discovered vulnerabilities. Organizations need clear mechanisms for researchers to report vulnerabilities directly to the appropriate party, and researchers need confidence that legitimate reports will be received, reviewed, and acted upon. Vulnerability disclosure programs (VDPs), bug bounty programs (BBPs), and coordinated vulnerability disclosure processes already provide these pathways and should remain the foundation for reporting as AI-enabled discovery continues.

These processes, however, need to adapt as AI increases the scale of discovery. HackerOne's experience as a launch partner in [Patch the Planet](#) provides one example of how existing vulnerability coordination infrastructure can support AI-enabled discovery at greater scale. Through the partnership, AI-assisted security research and validation is paired with expert

human review and established disclosure processes to help move vulnerabilities from discovery toward remediation. HackerOne provides the shared intake, triage, and tracking infrastructure through the H1 Platform, allowing researchers and maintainers to manage vulnerability reports, track remediation, and coordinate disclosure.

HackerOne's experience with Patch the Planet highlights an important point: scaling vulnerability discovery also requires scaling the infrastructure around it. More findings are only useful if they can be efficiently received, triaged, routed to the appropriate party, tracked, and moved through the remediation and disclosure process. Not every vulnerability will follow the same path. Depending on the finding, the party best positioned to act may be an affected vendor, an open-source maintainer, an existing disclosure program, a sector-specific coordinator, or another entity. Effective dissemination requires the ability to direct vulnerability information to the appropriate stakeholders efficiently.

(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 and guidance already provide a strong foundation for vulnerability disclosure and handling. NIST SP 800-216² provides guidance for establishing federal vulnerability disclosure programs, while ISO/IEC 29147³ and ISO/IEC 30111⁴ provide established frameworks for vulnerability disclosure and vulnerability handling. NIST should continue to build on these frameworks rather than develop a separate set of disclosure standards for AI-discovered vulnerabilities.

HackerOne has long supported broader adoption of VDPs, including among federal contractors. This support is particularly timely given Executive Order 14412, *Securing the Nation Against Advanced Cryptographic Attacks*.⁵ The Executive Order directs the FAR Council, in consultation with CISA and NIST, to propose amendments to the FAR requiring covered contractors to implement VDPs consistent with NIST guidelines. The order also directs that those VDPs incorporate reports of cryptographic vulnerabilities, including testing for lack of encryption and the use of non-FIPS-approved algorithms.

NIST has an opportunity to strengthen the guidance that will support broader VDP adoption across the federal contractor community. As NIST works with the FAR Council and CISA, it should ensure that its guidance remains practical for the organizations that implement

² NIST Special Publication 800-216, *Recommendations for Federal Vulnerability Disclosure Guidelines* (May 2023), <https://doi.org/10.6028/NIST.SP.800-216>.

³ ISO/IEC 29147:2018, Information technology – Security techniques – Vulnerability disclosure, International Standards Organization, Oct. 2018, <https://www.iso.org/standard/72311.html>.

⁴ ISO/IEC 30111:2019, Information technology – Security techniques – Vulnerability handling processes, International Standards Organization, Oct. 2019, <https://www.iso.org/standard/69725.html>.

⁵ White House, *Executive Order on Securing the Nation Against Advanced Cryptographic Attacks*, Section 6(d), June 22, 2026, <https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks>.

and operate these programs. That guidance should also account for the changing volume and types of reported vulnerabilities. In particular, guidance should help organizations establish clear processes for receiving reports, determining which reports warrant further review, ensuring they reach the appropriate security teams, communicating with researchers, and moving validated vulnerabilities toward remediation.

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?

As the number of identified vulnerabilities grows, organizations need better ways to determine which vulnerabilities require attention first. Prioritization should reflect actual risk and context rather than vulnerability volume or severity scores alone.

AI can help bring together information that would be difficult to analyze manually at scale. Relevant context may include exploitability, potential impact, affected products and systems, prevalence, available mitigations, and attack paths. AI may also help identify relationships between vulnerabilities, such as low-severity issues that can be chained into a more serious exploit.

HackerOne applies this type of contextual approach through the [H1 Platform](#), which brings together exploitability signals, attack-path analysis, and remediation intelligence to help security teams determine which exposures require attention. NIST should encourage prioritization approaches that account for real-world exploitability and operational context. AI can help surface and connect the information needed to make those decisions, but prioritization should ultimately be driven by the risk a vulnerability presents in practice, not by a severity score or automated output alone.

HackerOne has pursued several efforts aimed at improving risk assessment and prioritization:

- **H1 Validation** ([introduced](#) April 2026) combines agentic AI (AI that can carry out multi-step tasks on its own) with human security expertise to determine whether reported vulnerabilities are exploitable, provide remediation guidance, and separate real vulnerabilities from noise at scale.
- **H1 Remediation** [closes](#) the gap between finding a vulnerability and fixing it. It starts from findings already confirmed as exploitable, traces each one to the specific lines of code involved, and produces a developer-ready fix plan. That plan includes the root cause, suggested code changes, and implementation guidance. It can be sent to existing remediation tools or passed to an AI coding agent.

Together, these show how AI tooling can address the risk assessment and prioritization challenge. Automation lets teams work through findings and fixes at greater scale while focusing human experts on vulnerabilities that represent real security risk.

(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 operate as part of the broader vulnerability management ecosystem rather than as a standalone repository. Specifically, NIST should support open, machine-readable mechanisms that allow validated vulnerability information to move efficiently between the NVD, VDPs, vendors, and remediation workflows. Better integration with VDPs can reduce duplicative reporting, preserve useful technical context as a vulnerability moves through validation and remediation, and ensure that updates can flow between systems without requiring the same information to be manually re-entered. As vulnerability discovery scales, these connections will become increasingly important to moving actionable information efficiently from reporting to remediation.

7) Vision for the NVD

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

The NVD should continue to serve as a trusted source of vulnerability information while making it easier for relevant stakeholders to contribute additional information as understanding of a vulnerability evolves. A vulnerability record created at one point in time may not capture everything that later becomes known about exploitability, affected products, mitigations, or real-world impact.

To that end, NIST should establish mechanisms that allow vendors, vulnerability coordinators, security researchers, and other appropriate stakeholders to provide additional technical information or flag information that may be inaccurate or incomplete. Any such process should include appropriate safeguards for reviewing contributions and maintaining clear provenance so that users can understand where information came from and how it has changed.

For security researchers, clear expectations and feedback are particularly important. Researchers who provide useful vulnerability information should understand how that information will be handled and should have a visible path for supplying corrections or additional technical evidence. A process in which submissions receive no acknowledgement or

follow-up can discourage future participation and reduce the amount of useful technical information available to the broader ecosystem.

* * *

HackerOne appreciates NIST's continued leadership in strengthening the NVD and the opportunity to provide input. As AI increases the speed and scale of vulnerability discovery, the systems and processes that support vulnerability management will need to evolve alongside.

NIST has an opportunity to ensure that this evolution strengthens what already works. AI can help the vulnerability ecosystem operate at greater scale, but technology alone will not solve the challenges created by increased discovery. Effective vulnerability management will continue to be guided by human expertise and rely on trusted disclosure processes, risk-based decision-making, and reliable vulnerability information that can reach relevant organizations quickly. HackerOne looks forward to continuing to work with NIST and the broader cybersecurity community toward that goal.