CVE AT A CROSSROADS:

A BLUEPRINT FOR THE NEXT 25 YEARS

NICK LEISERSON
BOB LORD
LAUREN ZABIEREK

OCTOBER 2025

IST Institute for SECURITY + TECHNOLOGY

CVE at a Crossroads: A Blueprint for the Next 25 Years

October 2025
Authors: Nick Leiserson, Bob Lord, Lauren Zabierek
Design: Taylor White

About the Institute for Security and Technology

Uniting technology and policy leaders to create actionable solutions to emerging security challenges

Technology has the potential to unlock greater knowledge, enhance our collective capabilities, and create new opportunities for growth and innovation. However, insecure, negligent, or exploitative technological advancements can threaten global security and stability. Anticipating these issues and guiding the development of trustworthy technology is essential to preserve what we all value.

The Institute for Security and Technology (IST), the 501(c)(3) critical action think tank, stands at the forefront of this imperative, uniting policymakers, technology experts, and industry leaders to identify and translate discourse into impact. We take collaborative action to advance national security and global stability through technology built on trust, guiding businesses and governments with hands-on expertise, in-depth analysis, and a global network.

We work across three analytical pillars: the **Future of Digital Security**, examining the systemic security risks of societal dependence on digital technologies; **Geopolitics of Technology**, anticipating the positive and negative security effects of emerging, disruptive technologies on the international balance of power, within states, and between governments and industries; and **Innovation and Catastrophic Risk**, providing deep technical and analytical expertise on technology-derived existential threats to society.

Learn more: https://securityandtechnology.org/

About the Secure by Design Initiative

The Institute for Security and Technology's (IST) Secure by Design Initiative (SBDI) is a multi-stakeholder effort to realign responsibilities for cybersecurity, laying the foundation for continued deployment of secure-by-design practices for current and emerging technologies. The initiative brings together leaders from government, industry, academia, and civil society to drive systemic changes in how software is built, deployed, and maintained. Our work is aligned around three lines of effort: 1) researching and developing policy proposals to drive adoption of secure-by-design principles; 2) supporting and strengthening the core institutions that enable the secure-by-design lifecycle; and 3) acting as the hub for industry, academia, non-governmental organizations, and governments across the globe for policy related to software security. Through research, advocacy, and collaborative programs, the SBDI is working to create a future where security is a fundamental design choice—not an afterthought.

Acknowlegments

The authors are grateful to the many individuals who contributed their time, perspectives, and expertise during development of this paper. We would particularly like to thank Æva Black, Joshua Corman, Jen Ellis, Jerry Gamblin, Mitch Herckis, Jay Jacobs, Devin Lynch, Francesca Spidalieri, Megan Stifel, and Leopold Wildenauer, all of whom reviewed the paper in their personal capacities.

We also appreciate the organizers of BSides Las Vegas, particularly Daemon Tamer and Ed Prevost, and CyberNextDC, particularly Michael Daniel and Ari Schwartz, for the opportunity to share our ideas with a broader set of stakeholders.

This report is written and published in accordance with the Institute for Security and Technology's Intellectual Independence Policy. The authors are solely responsible for its analysis and recommendations. The Institute for Security and Technology and its supporters do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

About the Authors

Nick Leiserson is *Senior Vice President for Policy* at the Institute for Security and Technology. He previously served as a senior official at the White House Office of the National Cyber Director and as a Congressional chief of staff. He holds a degree in computer science from Brown University.

Bob Lord is *Senior Vice President for Digital Security Strategy* at the Institute for Security and Technology. Bob is a veteran cybersecurity executive and public-interest technologist. Most recently, he was a Senior Technical Advisor at the Cybersecurity and Infrastructure Security Agency (CISA), where he advanced efforts to make software that is secure by design. He was previously the first Chief Security Officer at the Democratic National Committee, where he helped secure the Committee and assisted state parties and campaigns in improving their security posture. Earlier in his career, Bob served as the CISO at Yahoo, the CISO in Residence at Rapid7, and as the first security hire at Twitter, where he built and led the information security program. You can find more about his interests at https://www.ilord.com.

Lauren Zabierek is *Senior Vice President for the Future of Digital Security* at the Institute for Security and Technology and a national leader in cybersecurity and technology policy. She previously served as Senior Advisor at CISA, where she co-led the Secure by Design movement to reduce systemic cyber risk. Her career spans the U.S. Air Force, civilian Intelligence Community, private sector, academia, and senior federal service, giving her rare insight into the decisions that shape digital security and resilience. She co-founded #ShareTheMicInCyber, served as Executive Director of the Cyber Project at Harvard's Belfer Center, and has advised leaders across government and industry on strategic, technical, and policy challenges.

Contents

Executive Summary

The Common Vulnerabilities and Exposures (CVE) Program is at a crossroads. Since 1999, it has served as the canonical index of software vulnerability identifiers, a critical function in a world that increasingly relies on software to power every aspect of modern life. Its success over the last quarter century is a testament to the vision of its founders and the dedication of the volunteers who have helped it grow into a core element of global software security.

However, recent funding and contracting issues have laid bare fundamental challenges with the program. Without adaptation, the vulnerability identification landscape will fragment. A quarter-century's progress driving towards a common lexicon will be undone. Cyber defenders will suffer as the task of deciphering what vulnerability an alert refers to falls on their shoulders. And software makers will lose a vital source of data about the prevalence of software defects, important information to drive progress in security-by-design.

To prevent fragmentation, the CVE Program must evolve. It needs a broader base of funding from governments, philanthropies, and industry. And it needs a new governance structure with representation from non-U.S. governments and voices from across the entire community of CVE Record producers and users.

This paper provides recommendations for global policymakers on how to reimagine the CVE Program for the next 25 years. At its core, it provides a policy framework that separates the creation and cataloging of universal vulnerability identifiers from other vulnerability management functions that rely on those identifiers. In particular, the paper calls for:

- **Global Vulnerability Catalog (GVC):** The GVC, a multistakeholder successor to the CVE Program, would "provide unique identifiers for and maintain and provide access to a catalog of actionable cybersecurity vulnerabilities." The existing CVE Record schema should be the starting point for GVC entries, and the catalog should preserve all existing data and identifiers that power global vulnerability management.

- **National (or Regional) Vulnerability Management Programs:** These programs would handle other key functions related to software vulnerabilities—beyond assigning identifiers—for both software producers and users. Using the Global Vulnerability Catalog unique identifiers and authoritative records, governments would then develop national or regional services tailored to their specific needs that build on this shared foundation. In practice, databases like the European Union Vulnerability Database are already structured this way, as they are based on CVE IDs.

The remainder of the paper focuses on the steps needed to create the GVC. Critically, policymakers must create a governance structure for the GVC that is more inclusive and transparent than that of the existing CVE Program.

As the sole funder of the CVE Program for its entire existence, the U.S. government is to be commended for its contributions to global cybersecurity. However, as a global, public good, other countries must step up to support the GVC, through funding and operational support. The paper provides concrete courses of action for global policymakers, led by the U.S. government, to create and sustain the GVC.

- The **White House Office of the National Cyber Director should, in partnership with CISA, engage in dialogue with their international counterparts**, as well as members of civil society and industry, about the development of a Global Vulnerability Catalog. These talks should be informed by Track 1.5 dialogues, supported by senior political leadership in participating governments, and focused on governance of the new catalog.
- The **United States Congress** should provide strategic direction to these efforts including by prioritizing funding certainty, committing to a multistakeholder successor to the CVE Program while invigorating a U.S. national vulnerability management program, and conducting hearings on the topic.

To enable these efforts, and in light of a lack of transparency about fundamental elements of the CVE Program, such as its annual operating budget or the status of its intellectual property, CISA should consider proactively making additional information about the CVE Program public.

To succeed, the GVC must also leverage the community of contributors who have helped to build the CVE ecosystem—especially the dedicated board members, many of whom have devoted thousands of hours to making cyberspace safer— to help guide the program's future. Policymakers should also lay out a clear set of milestones for the GVC, including objectives related to:

- **Data quality.** The GVC should focus on completeness, accuracy, and timeliness of CVE Records, enforced by strongly typed, machine-readable fields that adhere to a specified format and reject non-compliant inputs.
- **Modernization of the technical infrastructure that underpins the program.** Access to the database should be aligned with current technology standards and best practices, including cloud-native reliability, uptime guarantees, disaster recovery, and modern identity and access management.
- **A focus on customer use.** The GVC should prioritize approaches that support defenders in securing their systems today and that help software developers eliminate recurring classes of coding errors in the future.

At present, the CVE Program remains the most powerful tool available for tracking and measuring software security defects at scale. As it evolves into a Global Vulnerability Catalog, it must retain its status as a globally recognized and trusted reference point. This paper provides an updated governance and funding framework that reflects its role as a shared public good relied upon by stakeholders worldwide and ensures its continued success.

Introduction

Thanks to the tireless and passionate efforts of volunteers across the private sector, open-source communities, governments, and independent security researchers, the world for the last 25 years has been able to access a centralized catalog of software security defects: the Common Vulnerabilities and Exposures (CVE) Program. The CVE Program—which introduced for the first time a consistent numbering system—has served as the foundation for modern vulnerability management and enabled prioritization of and communication about software security flaws.

But the CVE Program is at a crossroads. Widely-publicized challenges with the contract that funds the program in spring 2025[1] have exposed its reliance on a single, U.S. government funding source. Furthermore, as cybersecurity regulations for operators have matured,[2,3] regulators in multiple jurisdictions—including the European Union (EU) through the NIS2 Directive and Cyber Resilience Act (CRA)—are relying on CVE Records as foundational inputs, raising more questions about CVE global governance and future interoperability. Finally, the proliferation in CVE Records filed in the catalog has produced a data quality crisis[4,5] that can no longer be papered-over by government-subsidized record "enrichment."[6]

These challenges have the real potential to undo a quarter century of progress. If stakeholders—particularly governments, but industry players as well—lose faith in the CVE Program, we could

[1] David DiMolfetta, "MITRE-backed cyber vulnerability program to lose funding Wednesday," *NextGov*, April 15, 2025, https://www.nextgov.com/cybersecurity/2025/04/mitre-backed-cyber-vulnerability-program-lose-funding-wednesday/404585/.

[2] The United States Food and Drug Administration (FDA) has released cybersecurity guidance clarifying responsibilities for device manufacturers both pre- and post-marketing. The guidance has specific requirements related to vulnerability monitoring, both in CISA's Known Exploited Vulnerabilities (KEV) Catalog and NIST's National Vulnerability Database (NVD); both are built on CVE. U.S. Food and Drug Administration, "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions," June 27, 2025, https://www.fda.gov/media/119933/download.

[3] The European Union's Directive (EU) 2022/2555 Network Information Security (NIS 2) Directive requires ENISA to the establish and maintain a creation European Vulnerability Database (EUVD), while the Cyber Resilience Act (CRA) obliges software providers to report actively exploited vulnerabilities and incidents via the Single Reporting Platform. EUVD itself is built on the CVE Program. European Parliament and Council, "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union," December 14, 2022, https://eur-lex.europa.eu/eli/dir/2022/2555.

[4] Cloud Security Alliance, "A Vulnerability Management Crisis: The Issues with CVE," November 21, 2024, https://cloudsecurityalliance.org/blog/2024/11/21/a-vulnerability-management-crisis-the-issues-with-cve.

[5] "CNA Scorecard: Tracking CVE Data Completeness," last accessed October 2025, https://cnascorecard.org/.

[6] The rapid rise in machine-generated code through the use of large language models (LLMs) could serve to exacerbate challenges with the volume of vulnerabilities. As of mid-2025, generative artificial intelligence models were seeing only marginal improvements in the security of the code they created. Yet they have both reduced the time it takes experienced software engineers to complete coding tasks and lowered the barrier of entry for creating working applications. While there may eventually be countervailing forces from LLM code review services, in the short term, the number of vulnerabilities is likely to increase. For more, see Veracode, "We Asked 100+ AI Models to Write Code. Here's How Many Failed Security Tests," July 30, 2025. https://www.veracode.com/blog/genai-code-security-report/.

see a fragmentation of numbering systems. Instead of having a single, authoritative index for referencing a particular vulnerability, we could have a multiplicity. Cyber defenders would suffer as they attempt to translate between different naming schemes—preventing them from being able to act quickly and with the most accurate information as they defend our digital borders from threats. At best, we would expend significantly more resources only to be left with a similar cybersecurity posture. At worst, vulnerabilities would slip through the cracks, resulting in more cyber incidents. In particular, impacts would fall on the most vulnerable entities worldwide—those actors with limited cybersecurity resources that underpin critical infrastructure in both the U.S. and abroad—and who increasingly find themselves targeted by cyber criminals and hostile nation-state actors.[7]

Faced with this prospect, it is time to refresh the CVE Program's governance structure and evolve its mission to help it succeed for the next 25 years. In this policy brief, we propose a framework for a Global Vulnerability Catalog that, when combined with national and regional vulnerability management programs, preserves the central promise of the CVE Program while allowing it to more nimbly modernize, address the concerns of its customers, and stand on a firmer foundation.

CVE: The What and Why

History

To understand the history of the CVE Program, one must first understand how vulnerabilities were classified before it came into existence in 1999. In Mann and Christy's foundational 1999 paper that introduced CVE,[8] they adroitly sum up the challenge:

> "Consider the problem of naming vulnerabilities in a consistent fashion. For example, one vulnerability discovered in 1991 allowed unauthorized access to NFS file systems via guessable file handles. In the ISS X-Force Database, this vulnerability is labeled nfs-guess; in CyberCop Scanner 2.4, it is called NFS file handle guessing check; and the same vulnerability is identified (along with other vulnerabilities) in CERT Advisory CA-91.21, which is titled SunOS NFS Jumbo and fsirand Patches. In order to ensure that the same vulnerability is being referenced in each of these sources, we have to rely on our own expertise and manually correlate them by reading descriptive text, which can be vague and/or voluminous."

[7] U.S. Cybersecurity and Infrastructure Security Agency, "Target Rich, Cyber Poor: Strengthening Our Nation's Critical Infrastructure Sectors," January 7, 2025, https://www.cisa.gov/news-events/news/target-rich-cyber-poor-strengthening-our-nations-critical-infrastructure-sectors.

[8] David E. Mann and Steven E. Christey, "Towards a Common Enumeration of Vulnerabilities," The MITRE Corporation, January 8, 1999, https://www.cve.org/Resources/General/Towards-a-Common-Enumeration-of-Vulnerabilities.pdf.

The CVE Program exists to ensure that cyber defenders understand which vulnerabilities they're referring to. At its heart, the program creates CVE Records that contain essential information about vulnerabilities and assigns them CVE numbers, which act as a universal identifier that can in turn be leveraged by the entire cybersecurity ecosystem.

Since its inception, the program has been funded by the United States government and operated by a Federally-Funded Research and Development Center operated by the MITRE Corporation. As software has become integral to every aspect of our economy, the program has grown significantly, from handling dozens of vulnerabilities to tens of thousands. This growth necessitated a federated approach to CVE Records: with such a proliferation of defects, no single person or entity could oversee their creation. Today, over 450 CVE Numbering Authorities (CNAs)[9] have the power to create CVE Records provide the canonical identifiers for vulnerabilities. These CNAs are typically software manufacturers but can also include open-source software maintainers, Computer Emergency Response Teams/Computer Security Incident Response Teams (CERTs/CSIRTs), and security researchers.[10]

The Value of the CVE Program

When Mann and Christy introduced the concept of CVE in 1999, cyber defenders were already using scanning tools to identify vulnerabilities within systems. In the decades since, that approach has only accelerated.

Today, defenders rely on CVE data both directly and indirectly to protect their systems. Directly, they review individual CVE entries to understand a specific vulnerability and assess its relevance to their environment.[11] Indirectly, defenders depend on a wide range of vulnerability management tools[12] that ingest and process CVE Records to provide prioritized guidance based on their organization's unique risk profile. This reliance is not limited to one geography—organizations across the globe, from small operators of essential services to multinational vendors and critical infrastructure providers, integrate CVE identifiers into their daily defense practices.

With the help of automation, these tools can correlate the ever-growing stream of CVE Records with an organization's asset inventory, highlighting which systems are vulnerable and which

[9] "CVE Numbering Authorities (CNAs), CVE.org, last accessed October 2025, https://www.cve.org/ProgramOrganization/CNAs.

[10] For more on the process to create a CVE Record, see Appendix I.

[11] Those assessments can lead to differing analyses about prioritization. Ankur Sand, Syed Islam, Michael Davis, Joshua Tigges, Marty Grant, and Rusty Clark, "The CVSS Deception: How We've Been Misled on Vulnerability Severity," presentation, Blackhat Europe 2024, December 11, 2024, https://www.blackhat.com/eu-24/briefings/schedule/#the-cvss-deception-how-weve-been-misled-on-vulnerability-severity-42509.

[12] "What are vulnerability assessments?" Gartner Peer Insights, last accessed October 2025, https://www.gartner.com/reviews/market/vulnerability-assessment.

exposures are most urgent to address. In real-world environments where defenders must make difficult tradeoffs between which updates to prioritize, this capability is essential. Applying every available update immediately is rarely possible due to operational constraints, system dependencies, or testing requirements.[13] Effective use of CVE data enables defenders to focus limited resources where they can have the greatest impact, reducing the likelihood of compromise while maintaining business continuity.

But the existence of a singular vulnerability database is no longer solely a capability leveraged by defenders for tactical cyber defense. It also plays a strategic role in advancing our understanding of the broader software ecosystem by highlighting the classes of coding error that are most common and the types of products they appear in. This insight gives the software industry a valuable opportunity to eliminate entire defect classes through better software development practices and the adoption of safer technologies. A key enabler of this strategic value is the inclusion of Common Weakness Enumeration (CWE) identifiers in CVE Records, a standardized taxonomy of recurring coding flaws.[14] CWE data equips stakeholders across the ecosystem with a clearer view of systemic product safety risks, supporting more informed decisions in areas ranging from software design to procurement policy. In this way, the CVE Program serves as a core datastream for initiatives to encourage the development of trusted technology that is secure by design.

Challenges

The creation and growth of the CVE Program over the past 25 years represent a major achievement in global software security. However, the program also faces real challenges that risk unwinding the unified classification system. Following the April 2025 uncertainty over the continuation of the program's funding, U.S. policymakers have paid increased attention to the program,[15] and rightly so—without a change of course, we could very well witness a fragmentation of the global vulnerability identification landscape.[16]

[13] "2024 Data Breach Investigations Report," Verizon, May 1, 2024, https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf.

[14] "CWE," last accessed October 2025, https://cwe.mitre.org/.

[15] "Ranking Members Thompson and Lofgren Request GAO Review of CVE and NVD Federal Cybersecurity Programs," press release, House Committee on Homeland Security, June 11, 2025, https://democrats-homeland.house.gov/news/correspondence/ranking-members-thompson-and-lofgren-request-gao-review-of-cve-and-nvd-federal-cybersecurity-programs.

[16] Interest in the program following the public funding flare up was not limited to U.S. policymakers. Yosry Barsoum, vice president and director at the Center for Securing the Homeland at MITRE, said at the time: ""We appreciate the overwhelming support for these programs that have been expressed by the global cyber community, industry, and government over the last 24 hours." Raphael Satter, "In last-minute reversal, US agency extends support for cyber vulnerability database," *Reuters*, April 16, 2025, https://www.reuters.com/world/us/us-agency-extends-support-last-minute-cyber-vulnerability-database-2025-04-16/. ENISA also noted it had been in conversation with MITRE in its press release announcing the EUVD. "Consult the European Vulnerability Database to enhance your digital security!," press release, European Union Agency for Cybersecurity, May 13, 2025, https://www.enisa.europa.eu/news/consult-the-european-vulnerability-database-to-enhance-your-digital-security.

Funding

In mid-April 2025, press reports emerged that the Department of Homeland Security (DHS) contract with MITRE supporting the CVE Program was at imminent risk of lapsing due to administrative delays. MITRE warned that the program would be suspended without immediate action by the government. The Cybersecurity and Infrastructure Security Agency (CISA) and DHS resolved the contracting issue that led to these warnings within days, and the program is, as of the time of writing, under contract through March 2026. However, the potential for the program to stop suddenly caused a diverse array of stakeholders to voice concerns.

Central to these concerns is the fact that the program relies on a single sponsor: CISA. Without a diversified funding stream—and with no reserve funds to speak of—the program is at high risk of operational disruption if that funding stream is reduced or redirected. Press reporting has indicated that contracts across DHS have been delayed as the new Secretary realigns departmental priorities.[17] Civil servants at CISA have since expressed their commitment to supporting the CVE Program and have announced interest in exploring alternative funding models,[18] but CISA has not announced a concrete plan for funding beyond March 2026.

The challenges with CVE Program funding come only a year after funding challenges with the U.S. National Vulnerability Database (NVD), maintained by the National Institute for Standards and Technology (NIST) and discussed in more detail elsewhere, when a contract for staffing support to enrich records in the NVD lapsed in early 2024. While NIST eventually found additional funding to restart that activity, the NVD's backlog has still not been processed.[19]

Programmatic

Beyond acute funding challenges, there are also several programmatic and operational concerns that stakeholders have raised about the CVE Program.

Transparency

MITRE—and by extension, CISA—have not been transparent about core elements of the CVE Program. The sudden revelation that the program could shut down shocked many members of the cybersecurity ecosystem. There is little publicly-available information about the budget

[17] Maxine Joselow, Alexandra Berzon, and Eli Murray, "Noem's Spending Rule Causes Delays at Homeland Security Dept.," *The New York Times*, August 21, 2025, https://www.nytimes.com/2025/08/21/us/kristi-noem-spending-contracts-homeland-security-department.html.

[18] U.S. Cybersecurity and Infrastructure Security Agency, "CVE Quality for a Cyber Secure Future," factsheet, September 10, 2025, https://www.cisa.gov/sites/default/files/2025-09/CISA_Common_Vulnerabilities_and_Exposures_CVE_Program_Vision-v6_CLEAN.pdf.

[19] Tanya Brewer and Matthew Scholl, "The National Vulnerability Database: VulnCon Update," presentation, VulnCon, April 10, 2025, https://www.first.org/resources/papers/vulncon25/VulnCon25-TBrewer-NVD-slides-final.pdf.

of the CVE Program, and current members of the CVE Board have expressed frustration about their lack of access to information about the inner workings of the program, including funding.[20] While the number of CNAs has expanded rapidly in the past decade, it remains unclear how the program adjudicates requests to become a CNA, including the degree to which the program exercises its discretion.[21] The program also has not set clear expectations for completeness of CVE Records, which has left actors like the NVD to "enrich" incomplete submissions up to a minimum viable standard.

All these issues point to a fundamental lack of transparency from the program. As an initiative that relies on voluntary submissions, maintaining trust among stakeholders is paramount to its continued success. Due in part to concerns around this lack of transparency, a group of current members of the CVE Board formed a separate CVE Foundation[22] in August 2024, which was publicly announced in the aftermath of the April 2025 funding concerns.

CVE Infrastructure

The CVE Program's infrastructure has not kept pace with the scale, complexity, or automation demands of today's software ecosystem. The core CVE submission and management systems remain fragmented, underpowered, and difficult to integrate into modern workflows.

The most widely used method CNAs use for submitting CVE Records is a volunteer-maintained HTML form hosted on GitHub that is not directly affiliated with or overseen by the CVE Program.[23] This form is designed for manual, single entry submissions and lacks features and infrastructure essential for enterprise-scale use.[24]

In addition to challenges with the submission process, the database itself provides only limited functionality for users. A lack of robust application programming interface (API) capabilities on cve.org, the CVE Program's website, prevents seamless, machine-to-machine integration of records with vulnerability management tools, bug bounty platforms, or vendor disclosure portals. As a partial workaround, CVE Records are also available in bulk form on GitHub, but this requires users to functionally build their own databases to make queries.[25] There exists no real-time or bidirectional synchronization between the CVE list, NIST's NVD, and other downstream

[20] Jonathan Greig, "Future of CVE Program in limbo as CISA, board members debate path forward," *The Record*, September 19, 2025, https://therecord.media/cve-program-future-limbo-cisa.

[21] This concern lies less with software producers looking to become a CNA for their own products. Rather, it is tied to non-software producers (e.g., researchers) or existing CNAs that have scopes broader than their own products. The CVE Program could provide additional clarity about trust and quality metrics for these types of CNAs, both new and existing.

[22] "CVE Foundation," last accessed October 2025, https://www.thecvefoundation.org/.

[23] Chandan B.N., "Vulnogram," last accessed October 2025, https://vulnogram.github.io/#editor.

[24] The CVE Program maintains its own submission form (https://cveform.mitre.org/), which is also antiquated and can result in CVE Records submitted to MITRE in its role as a CNA of Last Resort having significant data quality problems.

[25] "CVEProject / cvelistV5," last accessed October 2025, https://github.com/CVEProject/cvelistV5/tree/main/cves.

consumers. Instead, systems rely on periodic polling and manual reconciliation, leading to delays and inconsistencies.

Despite being the authoritative source for vulnerability identifiers, internet searches for CVE Record numbers often do not result in links to cve.org. Due largely to the design and implementation of cve.org, search results that point to cve.org are often ranked low in search engine results, appearing below vendor advisories, blog posts, and third-party aggregators—or sometimes not appearing at all. This undermines the program's credibility and utility as the definitive registry of vulnerability information. It also creates confusion for users seeking reliable, canonical sources. This is largely caused by the design and implementation of the CVE.org web site.

The long-term success of the CVE Program will depend on its ability to modernize its technical infrastructure. Given the ever-increasing volume and complexity of vulnerabilities, the program cannot rely on outdated tools, volunteer-maintained forms, or ad hoc processes. Modern vulnerability coordination requires modern infrastructure—built with robust APIs, real-time validation, transparent workflows, and scalable architecture. Without these improvements, the program will struggle to meet the needs of its contributors and consumers and to support the broader mission of reducing the dangers of unsafe software.

CVE Data Quality

The downstream value of the CVE Program depends on the quality and consistency of the data it provides. Yet many CVE Records are incomplete, vague, or formatted in ways that make them difficult to use in automated systems. Critical fields such as affected product names, version ranges, CWE tags, or remediation information are often missing or too loosely defined to support effective prioritization, correlation, or response.[26,27] This lack of completeness and accuracy undermines the ability of vulnerability management tools to function reliably, forcing tool developers and defenders to rely on guesswork or expensive manual verification and analysis.

A major contributor to this problem is the schema itself. Rather than enforcing structured, "strongly typed" fields—meaning fields that conform to a specified format—the current format allows arbitrary text in many places. As a result, CNAs can submit CVE Records that are formally accepted into the system, even when those records do not provide required information in a standardized manner. This flexibility creates downstream burdens for tool vendors, software bill of materials (SBOM) processors, and defenders who need to map vulnerabilities to real-world assets.

[26] Bob Lord, Jack Cable, and Lauren Zabierek, "Categorically Unsafe Software," blog, U.S. Cybersecurity and Infrastructure Security Agency, May 13, 2024, https://www.cisa.gov/news-events/news/categorically-unsafe-software.

[27] "CNA Scorecard: Performance Trends," last accessed October 2025, https://cnascorecard.org/trends.html.

Similarly, the current system does not allow a user to reliably surface all known vulnerabilities and weaknesses associated with a product. While this limitation is tied to well-documented issues with CVE Record quality at the time of creation, the CVE schema, and the Common Platform Enumeration (CPE) identifier system,[28] the resulting effect is that it hinders efforts to incentivize "security by demand"[29] by making it harder for buyers to assess product quality. Because software quality is difficult to measure, buyers need authoritative, product-level information to inform procurement decisions. Improving product searchability and linking CVE Records more directly to specific products would help bridge this gap and empower more secure purchasing decisions.[30]

Vulnerability Coverage

The evolving software landscape—and the emergence of large language models—have exposed several gaps in the CVE Program's coverage of vulnerabilities. These range from the immediate to the more speculative, but, in all cases, the lack of clarity from the program opens software users up to more risk.

» **Open-source Software.** Despite the significant growth in the number of CNAs, open-source software developers continue to be under-represented. As a result, open-source developers (and security researchers examining open-source projects) often face more friction when creating a CVE Record, which can reduce transparency. This can lead to issues like silent patching, when a developer discovers a vulnerability and fixes it internally without documenting it.

» **Operational Technology/Industrial Control Systems/Internet of Things.** The CVE Program grew out of traditional enterprise IT network defense. As a result, connected devices are under-represented within the program, both in terms of the vulnerabilities in the catalog that are associated with connected devices and the presence of manufacturers as CNAs. The unique consequences that can occur when operational technology is disrupted, particularly with respect to public health and safety—suggest that the program should do more to address this gap.

» **Cloud Vulnerabilities.** The CVE Program was not designed with the cloud in mind. Vulnerability fixes that did not require user action were often considered outside the scope of what a CNA was

[28] The SBOM Forum, "A Proposal to Operationalize Component Identification for Vulnerability Management," September 13, 2022, https://owasp.org/assets/files/posts/A%20Proposal%20to%20Operationalize%20Component%20Identification%20for%20Vulnerability%20Management.pdf.

[29] "Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem," fact sheet, U.S. Cybersecurity and Infrastructure Security Agency, August 2024, https://www.cisa.gov/resources-tools/resources/secure-demand-guide.

[30] Improved data quality could also facilitate alignment with regulatory requirements, such as those under the EU CRA and NIS2, where accurate and searchable vulnerability data directly support coordinated vulnerability disclosure, compliance reporting, and procurement policy.

expected to report. Despite the explosion of cloud offerings, cloud providers have been inconsistent in reporting vulnerabilities that require risk assessments from users, rather than direct action.[31,32]

- **AI.** Large language models and other machine learning technology may present unique risks of exploitation. In addition to vulnerabilities in the underlying software that resemble more traditional defects currently cataloged in CVE Records, the models may also be vulnerable to novel techniques such as prompt injection. While the CVE Program has blogged about the issue and created a working group on AI,[33] it has not articulated a clear strategy or preference about whether to catalog these unique types of vulnerabilities.[34]

Governance Gaps and Strategic Risks

These challenges point to two core governance issues: a lack of clearly defined roles and responsibilities for the players in the CVE ecosystem and an unclear delineation of the CVE Program's mission relative to other vulnerability management programs at the national and regional level that make use of CVE Records. While these issues have not prevented the CVE Program from providing value over its first 25 years, they present an acute challenge to the future of the program. Without clarity on these governance gaps, the program will struggle to address its most pressing need: diversified and sustainable funding. What's more, failing to evolve the CVE Program's governance model in line with its foundational role in software security means the programmatic challenges outlined above will likely continue. This ultimately risks the fragmentation of vulnerability cataloging across jurisdictions, which will undermine progress in vulnerability management and increase operational friction for cyber defenders.

Roles and Responsibilities

Many different entities play a role in the CVE ecosystem. Important players include:

- Cybersecurity defenders, who directly consume CVE Records while protecting systems.

[31] The CVE Program's original guidance stated that cloud vulnerabilities are in scope if remediation requires user action: "Dispelling the Myth: CVE ID Assignment and Record Publication for Vulnerabilities Affecting Cloud Services," CVE Program, September 13, 2022, https://www.cve.org/Media/News/item/blog/2022/09/13/Dispelling-the-Myth-CVE-ID.

[32] But subsequent updates to the CNA operational guidance now include vulnerabilities that only require users to conduct a risk assessment. While some cloud providers, such as Google, have stated they will file CVEs for vulnerabilities that do not require user action, coverage varies. "Google Cloud deepens its commitment to security and transparency with expanded CVE program," blog, Google Cloud, November 11, 2024, https://cloud.google.com/blog/products/identity-security/google-cloud-expands-cve-program.

[33] "CVE Program Adds New 'CVE Artificial Intelligence Working Group (CVEAI WG),'" CVE Program, October 15, 2024, https://www.cve.org/Media/News/item/news/2024/10/15/New-CVE-Artificial-Intelligence-Working-Group.

[34] The Program has published two blog posts outlining potential challenges with AI-related vulnerabilities that do encompass prompt injection. However, the CWEs mentioned in the blog are currently associated with only two CVE Records in the entire database. It may be that more clarity will emerge over time, but the current guidance remains unclear: "CVE ID Assignment and CVE Record Publication for AI-Related Vulnerabilities," CVE Program, February 18, 2025, https://www.cve.org/Media/News/item/blog/2025/02/18/CVE-ID-CVE-Record-AIrelated-Vulnerabilities.

- Cybersecurity tool makers, who use CVE Records to build scanning capabilities to identify vulnerable software.
- Academics and data scientists, who rely on CVE Records to better understand the state of software security and use data to predict attacker and vendor trends and exploitability.
- Security researchers, who discover and report vulnerabilities that become CVE Records.
- Beyond these classes of contributors, there are also organizations that more formally support or draw on the CVE Program.

CISA

In recent years, some have noted that CISA has attempted to exert more control over the CVE Program. As the sole fiscal sponsor of the CVE Program, it should not be surprising for CISA to want a strong say in the program's direction. However, members of the software security ecosystem, including CVE Board members,[35] have expressed strong and consistent pushback to CISA's attempts to exert influence over the program, including through its two-page vision statement, released in September 2025.[36] This friction speaks to a continued lack of clarity about the role of CISA—and the U.S. government more broadly—in the program. This significant mismatch in expectations regarding what CISA's role is and what it should be is a gap that policymakers must address.

MITRE

As the current CVE Program Secretariat, MITRE provides administrative, logistical, and operational support.[37] Its activities include:

- Hosting and maintaining the CVE website and database infrastructure
- Onboarding and managing CNAs
- Administering CVE Record policies and procedures
- Facilitating CVE Board operations, including meeting logistics and agenda-setting
- Chairing some working groups and maintaining program documentation

MITRE plays a central role in shaping how the CVE Program functions day to day. While the CVE Board, as discussed below, provides strategic input, MITRE controls the program's processes and maintains most of the tooling and infrastructure.

[35] Jonathan Grieg, "Future of CVE Program in limbo as CISA, board members debate path forward," *The Record*, September 19, 2025, https://therecord.media/cve-program-future-limbo-cisa.

[36] U.S. Cybersecurity and Infrastructure Security Agency, "CISA Presents Vision for the Common Vulnerabilities and Exposures (CVE) Program," press release, September 10, 2025, https://www.cisa.gov/news-events/news/cisa-presents-vision-common-vulnerabilities-and-exposures-cve-program.

[37] Chris Levendis, "Common Vulnerabilities and Exposures (CVE): Scaling Through Federation and Partnership," Software and Supply Chain Assurance Winter Forum 2023, MITRE, January 25, 2023, https://csrc.nist.gov/csrc/media/Presentations/2023/common-vulnerabilities-and-exposures/Jan-25-2023-ssca-levendis.pdf.

CISA sponsors the CVE Program through the Homeland Security Systems Engineering and Development Institute (HSSEDI), a Federally Funded Research and Development Center (FFRDC)[38] operated by MITRE. According to MITRE, CISA contracts with MITRE "to operate the CVE Program in cooperation with industry, government, and academic stakeholders under a public/private partnership."[39] However, it is unclear whether MITRE should continue to serve as the operational manager of the CVE catalog. While development of the CVE system was clearly within the remit of an FFRDC, successfully maintaining the global catalog and ensuring the underlying infrastructure keeps pace with operational requirements may ultimately fall outside the HSSEDI's mission.

CVE Board

According to MITRE, the CVE Board "is responsible for the strategic direction, governance, operational structure, policies, and rules of the CVE Program."[40,41] Its stated responsibilities in the Board Charter are "to work with each other and the community to oversee the program, provide strategic direction, and advocate for the CVE Program."[42]

These statements of the Board's responsibilities imply that it exerts management control. Indeed, the Board has exercised strategic leadership on numerous occasions throughout the history of the program, including devising and implementing the federated CNA model[43] that has allowed for the exponential growth of the program. However, as a creation of MITRE, the Board is fundamentally advisory in nature. It has no distinct legal standing of its own, and it lacks the authority to compel MITRE to make changes—it can only recommend them. The disconnect between the stated responsibilities of the Board and its ability to carry out those responsibilities is a clear gap in the existing program structure.

The Board charters and oversees working groups that focus on key areas like automation and quality. For example, the Board established the Automation Working Group (AWG) and the Quality Working Group (QWG) to help improve tooling and record consistency. However, while they are taking feedback from stakeholders and making suggestions, they do not have

[38] FFRDCs meet some "special long-term research or development need which cannot be met as effectively with existing in-house or contractor resources." "35.017 Federally Funded Research and Development Centers," FAR FAC 2025-26, effective October 1, 2025, https://www.acquisition.gov/far/35.017.

[39] "Frequently Asked Questions (FAQs)," CVE Program, last accessed October 2025, https://www.cve.org/ResourcesSupport/FAQs.

[40] "Board," CVE Program, last accessed October 2025, https://www.cve.org/ProgramOrganization/Board.

[41] "CVE: 25th Anniversary Report," CVE Program, October 2024, https://www.cve.org/Resources/Media/Cve25YearsAnniversaryReport.pdf.

[42] "CVE Board Charter," version 3.5, CVE Program, July 2, 2024, https://www.cve.org/Resources/Roles/Board/General/Board-Charter.pdf.

[43] Eduard Kovacs, "MITRE Puts Rapid CVE Assignment Pilot on Hold," *SecurityWeek*, March 21, 2016, https://www.securityweek.com/mitre-puts-rapid-cve-assignment-pilot-hold/.

the ability to implement change directly, particularly with respect to technical or operational requirements.

The Board has no terms for full members,[44] and several individuals have served continuously since the program's inception in 1999. While this continuity preserves institutional memory, it is an uncommon board governance practice and has the potential to lead to insularity. Board seats are held indefinitely, and members are not subject to re-election. In practice, full members largely remain until they voluntarily step down.

A further challenge is the limited representation of international stakeholders and key CNAs on the Board—for example, actors such as the European Union Agency for Cybersecurity (ENISA) which manages the EUVD, and comparable authorities in other jurisdictions are not formally included. This lack of international participation risks undermining the Board's global legitimacy and could make interoperability with regional or national vulnerability databases more difficult.

While the Board may be publicly perceived as controlling the direction of the program, formal authority rests with MITRE, potentially guided by direction from CISA. Clarifying the advisory nature of the Board—or actually empowering it to oversee the program—will be essential for the program's future.

CNAs

For much of the CVE Program's history, MITRE decided whether and when to create a new CVE Record for a particular software flaw. However, that responsibility is now given over to CNAs, which—largely voluntarily—adjudicate and then create CVE Records within their scope. The CVE Program could not function without the 450+ CNAs, which form the backbone of the federated model in use today. CNAs use a hierarchical model with four levels:

- » **CNA Top-Level Root:** There are two CNA Top-Level Roots, CISA and MITRE, which are responsible for managing their own hierarchies within their scope and holding CNAs accountable to agreed upon practices.
- » **Root:** There are seven Root CNAs responsible for recruiting and managing other CNAs within their hierarchies.[45]
- » **CNA of Last Resort**: A CNA of Last Resort is authorized to assign CVE IDs and publish records for vulnerabilities that are within their scope and not within the scope of a more specific CNA.
- » **CNA**: A CNA has a specific scope (a subset of their Root's scope) for which they can assign CVE IDs and publish CVE Records.

[44] "CVE Board Charter," version 3.5, CVE Program, July 2, 2024, https://www.cve.org/Resources/Roles/Board/General/Board-Charter.pdf.

[45] The two under the CISA Top-Level Root are CISA-ICS and CERT@VDE. The five under the MITRE Top-Level Root are Google, INCIBE, JPCERT/CC, Red Hat, and Thales Group,

NIST NVD

NIST operates the National Vulnerability Database (NVD), a separate system created in 2005 that ingests CVE Records from the cve.org database and then supplements them with additional data, including:[46]

- Common Weakness Enumeration (CWE) tags
- Common Platform Enumeration (CPE) identifiers
- Common Vulnerability Scoring System (CVSS) severity scores
- Additional metadata and references

Although NIST does not play a role in CVE creation, it is a downstream consumer whose work significantly affects how vulnerabilities are prioritized and remediated across the private and public sectors. Many individuals and organizations access CVE Records through the NVD, which has led some to believe that the CVE Program and the NVD are one and the same.[47]

NVD uses the word "enrichment" to describe its activities. While that word conveys the general idea that someone is adding new information, it also suggests that this information is a value-add to the base CVE Record that might be outside the purview of the CNAs and software producers. A different framing would be to say that the NVD upgrades CVE Records up to a "minimum viable" CVE Record. The minimum viable CVE Record framing then invites the question of which entity is best positioned to provide information about a vulnerable product: should that responsibility rest upon government analysts conducting third-party research, or might it be more efficiently completed by the creators of the product or software package themselves (or their designees)?

Other Vulnerability Databases

There are a multitude of other vulnerability databases around the world. Many use CVE IDs for indexing and interoperability purposes; some, like the European Union Vulnerability Database (EUVD) or the NIST NVD, are required to by policy. Of those built on the foundation of CVE, many are meant to be relatively comprehensive, encompassing a large number of vulnerabilities with CVE Records, but also adding in additional types of vulnerabilities that do not fit the CVE schema (e.g., the Open Source Vulnerability Database[48]). Some also provide further enrichment; for instance, CISA's Known Exploited Vulnerabilities (KEV) catalog comprises vulnerabilities that CISA has determined are actively being exploited in the wild.

[46] "CVE FAQs," NIST National Vulnerability Database, created September 20, 2022, updated June 27, 2024, https://nvd.nist.gov/general/FAQ-Sections/CVE-FAQs.

[47] Becky Bracken, Trey Ford, Adam Shostack, and Brian Martin, "Dark Reading Confidential: Funding the CVE Program of the Future," *DarkReading*, July 31, 2025, https://www.darkreading.com/cybersecurity-operations/funding-cve-program-future.

[48] "OSV," last accessed October 2025, https://osv.dev/.

There are databases, however, that do not aim for interoperability with CVE. The recently created Global CVE (GCVE) Allocation System, operated by the Computer Incident Response Center Luxembourg (CIRCL), is backwards compatible with CVE, but it also allows for creation of new vulnerability records independent of the CVE Program, even for vulnerabilities that would be in scope for CVE.

While some functions (e.g., those of a regulatory nature) are better held as national (or regional) competencies, a singular index of vulnerabilities brings significant benefits for the cybersecurity ecosystem—and moving to multiple catalogs risks returning the community to the challenges of the 1990s. The GCVE team argues:

> “The main difference [between GCVE and CVE] is decentralization. GCVE introduces GCVE Numbering Authorities (GNAs), which are independent entities that can allocate GCVE identifiers without needing blocks pre-allocated from a central authority or adhering strictly to centrally enforced policies. The traditional CVE system typically relies on a more centralized structure for ID allocation and policy.”

The greatest benefit of the CVE Program [is] having a singular, global understanding of what we mean when we talk about a particular vulnerability.

While the idea of decentralization is commendable as a way of building resilience against funding shortfalls or loss of control over the program, moving away from a centralized model also defeats the greatest benefit of the CVE Program: having a singular, global understanding of what we mean when we talk about a particular vulnerability.[49]

Involving international stakeholders in the governance of the CVE Program is essential to alleviate concerns about centralization and control over the catalog, avoid the proliferation of more databases that do not link back to CVE IDs, and ensure that new databases—such as the EUVD—remain interoperable with CVE rather than diverging into parallel, incompatible systems that fragment the global vulnerability landscape.

Mission

Today, many of the key stakeholders in the CVE Program represent software producers. This is understandable, as it is largely producers who create CVE Records that arise from the vulnerabilities in the code they create—or who interact with a designated CNA to create those CVE Records. But commercial software companies, for example, already use their own, internal bug-tracking systems to keep tabs on defects in their own products. Software users

[49] Incidentally, a decentralized model also makes conflict resolution or de-duplication of vulnerabilities less likely, so fractured references can occur *within* a single decentralized system.

are the group who gain the most value from a catalog, as emphasized in Mann and Christy's 1999 paper outlining the CVE schema. The lessened emphasis on the downstream customers of CVE Records may be a contributor to present-day challenges with the CVE Program.

To realize the full value of CVE, entities across the entire lifecycle of a record—from the initial discovery of a vulnerability, to the assignment of a CVE ID, to the moment a defender uses that information to protect an environment in the most cost-effective way—must be considered and strongly represented in the program. Neglecting this downstream perspective risks optimizing for process rather than impact. Moreover, the extent to which downstream consumers can operationalize CVE information is an important indicator of the effectiveness of the CVE Program. A catalog of software defects is only as successful as its ability to be leveraged to reduce risk.

Over the last 25 years, the CVE Program has evolved from a technical tool to a strategic asset. Beyond providing operational utility to software users, the CVE Program can also help software producers and policymakers reduce risk stemming from those products in the first place.[50] By helping to link information from disparate vulnerability databases, the CVE Program provides invaluable insight about the state of software security across products and the industry. As the program evolves, its success should also be measured by how well it supports broader understanding of software.

[50] Peter Mell and Assane Gueye, "A Suite of Metrics for Calculating the Most Significant Security Relevant Software Flaw Types," 2020 IEEE 44th Annual Computers, Software, and Applications Conference, September 22, 2020, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=929586.

A Global Vulnerability Catalog (and National Vulnerability Management Programs)

It is time to consider how the vulnerability ecosystem should evolve in a way that builds on the success of the CVE Program, recognizes existing challenges, and plays a strategic role in the world's growing dependence on software. Persistent issues such as a lack of sustainable funding, transparency, and broad international participation highlight the need for a new model.

First and foremost, the next evolution of the CVE Program must adopt a new governance model that is both more inclusive and supports more sustainable funding from a more diverse array of stakeholders. In developing that new governance approach and the concomitant roles and responsibilities, policymakers need a framework to differentiate between the role of a singular, global catalog of software defects and the multitude of public and private databases that are built atop such a catalog.

We propose the creation of a Global Vulnerability Catalog (GVC) as a multistakeholder successor to the CVE Program. In our proposed model, the GVC would be leveraged by complementary national (or regional) vulnerability management programs (NVMPs).

A Global Vulnerability Catalog

As a starting point, consider the CVE Program's stated mission: to "Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities." That same mission should form the basis for a GVC, with some changes to help it reflect the current state of the software security ecosystem.

In considering what the mission statement for a proposed GVC should be, we suggest examining the following verbs:

» **"Identify"** is ambiguous. Is the CVE Program meant to identify vulnerabilities in software products? Or is it meant to provide unique identifiers for vulnerabilities? As discussed, the CVE Program's greatest value-add—and the reason for creating it in the first place—is providing a common index for vulnerabilities. We propose that the successor GVC should clarify its mission is to provide unique IDs for vulnerabilities.

» **"Define"** is similarly unclear. The elements of a CVE Record currently reside under the purview of the program. We do not propose giving them over to a standards developing organization. However, rather than describing its role as defining the elements that go into a vulnerability catalog, we suggest clarifying that the GVC's higher-level mission is to maintain the vulnerability catalog, rather than highlighting defining the contents of that catalog as a separate function.

- **"Catalog"** is insufficient as a verb. The value of a GVC comes from both having a unique identifier and providing the ability to access or look up vulnerabilities based on said identifier. Thus, the GVC should both maintain and provide access to a catalog of vulnerabilities.

As a practical matter, CVE Records are regularly reserved for vulnerabilities that have not yet been "publicly-disclosed," so that language is superfluous.

Finally, the word "vulnerability" in the CVE Program's mission statement warrants further review and clarification. What exactly is a vulnerability? As noted in the Challenges section, the program currently faces a spectrum of coverage challenges, including questions of program reach (are open-source software vulnerabilities sufficiently surfaced?) to ones of program scope (should vulnerabilities in LLMs that are the result of insufficient training, not coding error, be assigned CVE numbers?). In considering what constitutes a "complete" vulnerability, the program must clarify the minimum amount of data necessary for a catalog entry to be complete. The GVC will need to establish from the beginning whether the core CVE Record fields of identification number, product affected, brief description of the vulnerability, and link to public information are sufficient to constitute a "complete" vulnerability.

While this paper proposes a conceptual distinction between the GVC and national and regional vulnerability management programs, the actual demarcation between the two will be determined by the GVC's established mission from the start—any data field or vulnerability information that is beyond the requirements of the global database will, out of necessity, be left to other programs. This demarcation should be made explicit early on, both to avoid duplication of efforts and to provide clarity to jurisdictions with existing mandates—such as NIS2 and the CRA in the EU—on how the GVC interfaces with national or regional reporting and disclosure systems. The existing requirements for CVE Records should serve as a starting point for the GVC, but the conversation must be continued with ample consultation from stakeholders and room for iteration as the software ecosystem evolves.

For the purposes of the GVC's mission, the word "actionable" may help inform the minimum requirements for a catalog entry. While there may be significant value that other parties can provide (e.g., information about exploitation), the minimum for a complete entry should ensure that an individual examining a record has enough information to take action based on the data contained therein.

A GVC should then "provide unique identifiers for and maintain and provide access to a catalog of actionable cybersecurity vulnerabilities."

The proposed GVC is not intended to compete with the CVE Program but to serve as its natural evolution. This transition would establish the GVC as a new legal entity. The shift is fundamentally about governance: the new GVC board would take responsibility for setting policy and making programmatic decisions. To ensure continuity, all existing CVE Records would be incorporated, with the current CVE Record schema serving as the foundation for future GVC entries.

National (or Regional) Vulnerability Management Programs

There are many other key functions pertaining to software vulnerabilities on the software producer and the user side that go beyond providing identifiers and maintaining a catalog. We believe that those functions are not best handled through a single, authoritative catalog. Instead, we propose leaving them to competent national or regional authorities.[51]

These programs would not duplicate the global function of creating identifiers or maintaining the canonical record set. Instead, they would work with domestic businesses and government agencies to translate global data into actionable national priorities.

Examples of value-added roles include:

- Coordinating vulnerability disclosure with local software manufacturers
- Highlighting exploitation status specific to a given region
- Publishing indicators of compromise (IOCs) and attack patterns observed domestically
- Offering sector-specific guidance aligned with national regulation and industry needs
- Generating vulnerability metrics
- Localizing advisories and records into national languages
- Integrating vulnerability data with national threat intelligence and incident response systems
- Producing analytics and research to inform policy and private-sector planning
- Supporting workforce training and education to strengthen local capacity

The ideal outcome is for governments to rely on this new common global database for unique identifiers and authoritative records, while developing national or regional services that build on this shared foundation.[52]

[51] There are also non-governmental vulnerability management efforts, such as commercial vulnerability databases, that are out of scope for this report. Broadly speaking, all vulnerability management programs and databases benefit from a common identifier like CVE. Commercial vulnerability scanning and management solutions incorporate CVE—and the companies that make them are often CNAs themselves. Academic datasets and research also frequently cite CVE IDs and CVE data.

[52] Although national security or regulatory jurisdictional considerations may require some functions to be carried out at the national level, to the greatest extent possible, services should be harmonized (or regionalized to begin with) to avoid unnecessary duplication of effort.

This model already exists in practice. Countries such as Japan[53] and South Korea[54] operate national vulnerability management programs that reference CVE Records. While they may issue local identifiers as well, the link back to CVE Records ensures that every vulnerability can be described with a globally unique identifier, enabling defenders everywhere to communicate clearly. The EUVD has also taken this approach, using CVE identifiers as a global index while providing additional data—and leveraging entries for regulatory requirements.

From Here to There

Though we maintain that building effective national vulnerability management programs is critical to reducing the dangers from software vulnerabilities—a topic which warrants further discussion—for the purposes of this paper, we focus on the specific steps U.S. policymakers need to take to build a Global Vulnerability Catalog based on the existing CVE Program. These steps will only succeed, however, if they are developed with international partners in mind and designed for global adoption.

Governance

The most important change policymakers must effectuate is to create a governance structure for the GVC that is more inclusive and transparent than the existing CVE Program.

Multistakeholder

The software vulnerability ecosystem comprises a diverse array of stakeholders. To ensure that the GVC represents their perspectives, its governance structure must include a way for them to participate. This starts with governments all over the world, which are both most likely to fund this public good—and also most capable of setting up a competing system that would lead to a fracturing of the vulnerability identification ecosystem. The CVE Board currently contains representatives from only one government: the United States. This is not sustainable. Other governments committed to stability in cyberspace must have a voice in the operations of the GVC. This may include regional authorities such as ENISA, which manages the EUVD under NIS2, and comparable bodies in other jurisdictions.

Participation cannot be limited only to governments. Software producers, software users, security tool developers, and security researchers all make use of CVE Records, and their interests must also be represented in the operations of the GVC. In considering how to

[53] "Japan Vulnerability Notes," last accessed October 2025, https://jvn.jp/en/.

[54] "Korea Internet Security," last accessed October 2025, https://www.kisa.or.kr/EN/101.

integrate industry, academia, and civil society into GVC governance, policymakers could directly allocate board seats or form an advisory council, among other options. Above all, the chosen structure must encourage multistakeholder participation: the operations of the GVC will be fatally compromised unless non-governmental stakeholders help to drive the activities of the catalog.

Multiple Funding Streams

As well as expanding the pool of board members, policymakers must also ensure that the GVC is backstopped with a diverse array of funding mechanisms. The U.S. government has single-handedly subsidized the creation of the CVE Program, and it should be commended for its foresight and generosity in doing so. However, no single government should bear the responsibility for funding the GVC—nor should any single government have the control over the program that derives from control of the purse strings.

The most important change policymakers must effectuate is to create a governance structure for the GVC that is more inclusive and transparent than the existing CVE Program.

CVE, and by extension the proposed GVC, is a public good. As such, it is susceptible to the free rider problem. Software producers or users who derive value from the GVC may wish to contribute to it financially; however, it is likely that such contributions effectively subsidize their competitors, who also make use of the GVC. They are, therefore, unlikely to be fully incentivized to make such contributions. Of course, the alternative—that they are able to derive some competitive advantage from supporting the GVC—is even worse, as such an advantage would likely involve prejudicing the defects in the catalog in some way.

It is most likely that this type of benefit may be pursued by software suppliers. It is worth noting, however, that while software suppliers are not currently directly funding the program, many are already investing considerable resources into its operations through their activities as CNAs.

For consumers of CVE, there is less of a potential for a conflict of interest as their greatest benefit comes in the form of a clear, consistent, and reliable catalog, which should be a shared goal for CVE stakeholders across the whole ecosystem. There are many companies that rely on CVE as part of their internal security response program and that therefore may be willing to support the program’s continued operations. This form of funding may not be reliable as a renewed source of funding year over year, so it should not be viewed as primary funding. Rather, it may be an opportunity to diversify and enrich funding pathways and cement the shared ownership/responsibility of the CVE Program.

A diverse funding portfolio can include industry contributions so long as they are not overly concentrated (both within a given time period and over time) and are not tied in any way to outcomes from the program. A transparent, accountable, and disciplined governance structure is key for avoiding both actual conflict of interest and the appearance of such.

CVE, and by extension the proposed GVC, is a public good.

A more natural source of funding for public goods, though, is government and philanthropy—and financial support from an array of governments, in particular, will be critical to the GVC's success. International cost-sharing mechanisms should be explored so that stakeholders from outside the U.S. have both a financial stake and a governance role in the GVC's long-term success.[55]

Standard Practices

In creating a new governance model for the GVC, policymakers should focus on implementing standard practices, particularly:

- **Board Responsibility:** The GVC Board should have overall responsibility for the GVC. In particular, this includes a fiduciary responsibility, related to the efficient expenditure of revenues (including avoiding conflicts of interest), and an oversight responsibility, to ensure that the management team running the day-to-day operations of the GVC are fulfilling its mission. This contrasts with the current CVE Board, which, despite the title, is functionally advisory in nature.
- **Transparency:** A common critique of the CVE Program is that it is not transparent, whether about financial data or decision-making processes. Policymakers should ensure that there are clear requirements written into a GVC charter governing reporting to the public and holding it accountable. These could include annual reports that disclose data such as record volume and quality metrics and independent audits that assess the GVC across elements such as security posture and fairness, neutrality, and adherence to governance rules.
- **Board Composition:** Policymakers should also ensure that the board adheres to common governance practices, including having a fixed size, clear terms for members, and a definitive structure to guide the selection of new board members. Policymakers should also consider other matters such as whether to have ex officio members or term limits for board members.

Strategic Direction

Policymakers are primarily responsible for defining the governance structure and mission of the GVC. However, they can also provide strategic direction to the new program. When considering the strategic direction that a GVC should take, there are several elements that will be critical to its success.

[55] There are several models that policymakers could consider to help diversify revenue from governments, including dues tied to board representation or proportional assessments based on prevalence within the catalog.

Built on CVE

Most importantly, the GVC must leverage and carry forward the work of the CVE Program. At the bare minimum, that means that the GVC must contain all extant CVE Records at the time of its creation. In addition, the GVC, as the natural evolution of the CVE Program, will likely need to pick up the existing contract from the U.S. government as seamlessly as possible. The CVE infrastructure needs to be modernized, certainly, but there is no reason to delay improvements to governance pending operational changes.

Beyond the records and the systems that store them, it will be critical that the GVC also leverages the community of contributors to the CVE ecosystem to help guide the program's future. That includes existing board volunteers and open-source developers, many of whom have selflessly devoted thousands of hours to make cyberspace safer. While the structure of the CNA system will certainly be within the purview of the board to decide going forward, at present there is no reason to upend the federated model.

Plan for Transition

As a corollary to building on the existing CVE Program, policymakers should also include a transition period in any plan for the GVC. It may make sense, for instance, to eventually bring GVC program administration in-house, rather than contracting for it, as the U.S. government does today with MITRE. The GVC might also determine to bid out the contract to a specialty service provider. Regardless, in the immediate term, the focus should be on handing the CVE Program to new stewards, in the form of an empowered, international board, and then making structural reforms to its infrastructure and processes. Because the CVE Program is so integral to users' defenses, it is paramount to avoid any discontinuities in its operation. In weighing the tradeoffs, policymakers should prioritize a longer, more complete transition over a faster process that, although it can achieve a desired endstate quicker, has the potential to disrupt the identification and cataloging of software defects.

Policymakers might also want to consider how strategic communication will shape the transition from CVE to GVC. Given the public visibility of CVE and its global impact, it will be essential to acknowledge and address the diverse needs of stakeholders across government and industry, as well as the open-source and international communities. Transitions of this scale are not only technical, but also organizational and cultural, requiring careful attention to trust, legitimacy, and continuity. A well-managed shift can minimize disruption while laying the groundwork for broad adoption and long-term success.

Key Indicators of Success

Beyond these transition considerations, policymakers should also lay out a clear set of milestones for the new board. Key areas of focus for the GVC should include:

- **Data quality.** For the purposes of the CVE Program, "quality" is a function of CVE Record completeness, accuracy, and timeliness (CAT), terms that should be formally defined as part of a GVC strategic plan. CAT should be rooted in its operational context and should be informed by downstream software customer and manufacturer participation in stakeholder discussions. The GVC should move from free-form text fields to strongly typed, machine-readable records, meaning fields that conform to a specified format, such as date fields that require a specific date format and reject inputs that do not comply. It should establish minimum requirements for a viable vulnerability record56 and measure CNA performance against those norms.
- **Technology platform.** The GVC needs modernized web and API access to the program's database in line with current technology standards and best practices. This should include robust APIs, cloud-native reliability, uptime guarantees, disaster recovery, and modern identity and access management.
- **Downstream value.** Historically, the CVE Program has been oriented toward upstream record providers. Modernization should focus on how CVE Records support defenders in securing their systems today and how they help software developers eliminate recurring classes of coding errors. A key area of focus should be resolving identity issues, including how to easily represent the prevalence of CVEs in common software components like open-source libraries.

Pitfalls

There are two major risks tied to the evolution of the CVE Program. The most significant is the fragmentation of the software defect cataloging function across multiple disparate programs. The second is a regression in the number of participants, volume of reports, or quality of CVE Records due to changes in governance. While there are certainly many improvements that can be made to the existing program, changes should not come at the expense of what is working today. This section outlines three of the areas policymakers should keep in mind to minimize the chance of negative outcomes as the CVE Program evolves.

International Inclusivity

Throughout this paper, we refer to policymakers. Since our recommendations are for a Global Vulnerability Catalog, this is meant to be an inclusive term that encompasses governments committed to the stability and security of cyberspace the world over. However, as a practical matter, the first steps will likely need to be taken by a specific subset of policymakers, namely:

[56] In some cases, there will be a tradeoff between completeness, accuracy, and timeliness. In those cases, the GVC may decide to prioritize completeness and accuracy with the understanding that CNAs will make updates as they learn more. However, without more data about the processes software producers use today in creating CVE Records, the scope of this challenge is unclear.

U.S. political leadership in the Department of Homeland Security, White House Office of the National Cyber Director, and Congress.

This transition from a U.S.-led effort to a truly global one entails significant risk. From a U.S. perspective, policymakers should beware of fragmentation and a return to the pre-1999 state, the greatest risk to a canonical vulnerability cataloging system. While moving to a Global Vulnerability Catalog will necessarily mean ceding some control over the system (albeit control that the U.S. government has, to date, wisely refrained from exercising), it also presents an opportunity for the costs of the program to be spread across a much wider base. This is very consistent with the current Administration's approach to other global security organizations that meet U.S. policy objectives but that force U.S. taxpayers to foot a disproportionate amount of the bill.

From a global perspective, policymakers should similarly consider fragmentation the greatest risk to a canonical vulnerability cataloging system. Non-U.S. governments understandably want—and should have—more of a say in the operation of this critical cybersecurity infrastructure. At the same time, they must come to the table willing to make real investments to address the most acute need for CVE: diversified, stable funding. This must translate into both governance roles and tangible commitments—financial, technical, and operational—to sustain the GVC as a truly shared global resource.

As we have outlined in this paper, there exists a clear path forward for policymakers that results in a new, stable equilibrium with more consistent funding and a broader range of government voices steering vulnerability cataloging. However, without a relentless focus on the risk of disharmony and the dissolution of the existing identification regime, the pressures on policymakers, both U.S. and otherwise, to preserve or exert control may end up manifesting the fragmentation we fear.

Keeping the Catalog Focused

Many competencies related to vulnerability management are truly national competencies. A clear example is the use of a database for regulatory purposes. In the U.S., the KEV Catalog is used as the basis for patching requirements for Federal agencies. With the passage of the Cyber Resilience Act in the EU, software makers will have new obligations to report exploited vulnerabilities in their products to ENISA for inclusion in the EUVD. Our framework clearly delineates between the identification and cataloging responsibilities of the GVC and the added value that can come from national or regional vulnerability management programs. Were the focus of the GVC to move beyond identification and cataloging, that could present a significant risk that national or regional authorities could reject participation in the GVC over concerns it interferes with national prerogatives. It is critical to the success of the GVC to build a two-tiered model with a clear delineation of responsibilities between the singular, multistakeholder foundation and the diversity of governmental programs built atop it.[57]

Questions of Manufacturer Responsibility

The existing CVE "enrichment" process substitutes U.S. government contractors for software authors, entities who are generally in the best position to provide core CVE data.[58] This creates duplication of effort, uses taxpayer resources, and slows down the flow of critical information to defenders.

One of the most common objections to CNAs taking on the responsibility of ensuring CVE Records meet minimum standards is that they may lack the incentive to provide high-quality data. In some cases, the objection is not about incentives but about flaws in the way the Common Platform Enumeration (CPE) field is designed. The CPE specification leaves room for improvement. For example, it was developed before CVE Records were moved to a structured JSON format, which makes it appear outdated compared to other fields. CPE also relies on a centralized database of software authors and product names maintained by NIST. While that arrangement may have been sensible when CPE was first created, the dramatic expansion in the number of CNAs has rendered the model obsolete and in urgent need of redesign.[59]

Another concern about assigning these responsibilities to CNAs centers on assigning severity scores to vulnerabilities (such as a CVSS score[60]). Critics question whether downstream consumers can trust CNAs, particularly software manufacturers, to assign an accurate score to defects in their own products. They worry that vendors might downplay risks in order to minimize negative publicity.[61]

That concern deserves to be taken seriously, and it also raises further questions. Because the database is public, what would happen if a CNA routinely misrepresented CVSS scores? How would current and prospective customers or security researchers react if they saw repeated patterns of understatement from a vendor? The reputational and commercial consequences of being caught would likely outweigh any short-term benefit from downplaying risk. Having publicly-funded dashboards could amplify these incentives.

[57] The GVC should also clearly define the boundary between its mission and coordinated vulnerability disclosure (CVD), which primarily takes place in private channels before publication. While it is helpful for IDs to be decided before public disclosure, "full-scale" CVD requires substantially different capabilities than vulnerability cataloging.

[58] A security researcher who discovers a particular vulnerability might also have unique insights; however, assuming the use of a coordinated vulnerability disclosure process, that information should be passed to the software authors.

[59] The CPE record format also is incompatible with common practices in open-source software communities and therefore cannot be relied upon to accurately identify open-source components.

[60] "Common Vulnerability Scoring System SIG," FIRST, last accessed October 2025, https://www.first.org/cvss/.

[61] Regulatory or contractual requirements may, in fact, actively incentivize software creators to minimize the amount of data they provide, as vulnerabilities deemed "higher risk" may come with additional burdens related to reporting or remediation.

There is also little evidence that NVD's enrichment is more accurate than what CNAs could produce,[62] especially if the CNA is also the software's author. In fact, the opposite may be true: CNAs are often much closer to the software and therefore better positioned to provide complete, accurate, and timely data.

Next Steps

This paper proposes a natural evolution of the CVE Program into a multistakeholder Global Vulnerability Catalog, a distinct entity which can then be leveraged by complementary national and regional vulnerability management programs. If policymakers agree with the framework presented herein, there are several immediate steps they should consider to move the CVE Program onto a firmer foundation.

Dialogues with Other Governments

Concurrent with Congressional activity, the White House Office of the National Cyber Director should consider directing the interagency to engage in dialogue with their international counterparts, as well as members of civil society and industry, about the future of the CVE Program. These dialogues should prioritize the perspectives of international stakeholders whose systems already depend on CVE identifiers. In order for the talks to be effective, they must be:

- **Guided by track 1.5 conversations.** Industry and civil society are critical to the current—and future—success of the CVE Program, both with respect to governance and cataloging vulnerabilities. Track 1.5 conversations led by civil society organizations that feature leaders in the vulnerability management community can prevent misunderstandings between government and non-government stakeholders.
- **Operator-led.** Operational cybersecurity agencies like CISA and ENISA have the clearest equities in the Global Vulnerability Catalog—not least because they also have responsibilities for national vulnerability management programs that will be built atop the global catalog. However, while some governance discussions will likely need to be government-only, the success of a Global Vulnerability Catalog is predicated on bringing other stakeholders into governance as soon as possible.
- **Supported by senior political leadership.** Funding remains the most acute need for the program, and the support of global political leaders will be vital to ensure that diverse stakeholders bring money to the table.
- **Focused on governance.** There are clearly opportunities to further improve the CVE Program on a range of topics, from its infrastructure to its transparency. However, these programmatic changes are best addressed after the program is on firmer financial footing with a more diverse set of funders

[62] Julia Wunder, Alan Corona, Andreas Hammer, and Zinaida Benenson,"On NVD Users' Attitudes, Experiences, Hopes and Hurdles," ACM DTRAP Special Issue on IMF 2024, September 19, 2024, https://arxiv.org/html/2408.10695v2.

and directors. Focusing talks on governance avoids getting lost in details of program management that are best addressed by operational experts. At the same time, global participation in governance discussions from the outset will help prevent fragmentation and reinforce the trust needed within the broader CVE community.

Strategic Direction from the U.S. Congress

Since the April 2025 funding issue, members of Congress have publicly indicated their interest in addressing the future of the CVE Program, including by commissioning a formal audit by the Government Accountability Office. This strategic leadership is to be commended and is essential for the program's future stability. Vulnerability handling is critical to software security, and Congressional oversight—and, eventually, legislative oversight from other parliaments—is important to ensure stability of funding and continued buy-in from political leadership.

Leaders of the Congressional homeland security and science committees can further the evolution of the CVE Program by:

» **Prioritizing Funding Certainty.** The most acute challenge facing the CVE Program is ensuring there are no contracting challenges when the current tranche of funding ends in March 2026. Through the annual appropriations process, Congress should consider measures to ensure continuity of funding so that there is space to have broader conversations about the future of the program.

» **Committing to a Multistakeholder Model While Invigorating a National Vulnerability Management Program.** Public statements from elected officials in support of a multistakeholder Global Vulnerability Catalog could have a powerful impact on working-level negotiations about new governance models and funding structures. At the same time, Congress could consider codifying elements of a national vulnerability management program at CISA to address desired outcomes that are best addressed through national authorities.

» **Conducting Hearings.** As noted elsewhere, the CVE Program has a diverse array of stakeholders. Congressional hearings are an effective way to garner more perspectives on potential changes to the governance structure. Congress might also consider bringing in international stakeholders to reaffirm a commitment to a multistakeholder Global Vulnerability Catalog.

Transparency about Program Needs

This paper proposes one path forward that maintains a canonical, singular, and global vulnerability catalog while giving nation-states (and regional organizations) flexibility to develop additional programs atop it. While we are confident in the efficacy of this framework, there are other models that policymakers could consider (e.g., a purely non-governmental foundation). However, policy development and stakeholder engagement are severely hampered by the lack of transparency about fundamental elements of the CVE Program, such as its annual operating budget or the status of its intellectual property. To enable more constructive conversation about the next 25 years of successful vulnerability cataloging, CISA should consider proactively making additional information about the CVE Program public—or at the very least, clearly articulating legal restrictions that prevent it from doing so.

Conclusion

The CVE Program stands at a crossroads. Its success over the last quarter century is a testament to the vision of its founders and the dedication of the volunteers who have helped it grow into a foundational element of global software security. However, without evolving through more diversified funding and governance structures, it risks unwinding its greatest achievement: a single, canonical reference point for software security vulnerabilities. This reference point must remain globally recognized and trusted, requiring governance and funding models that reflect its role as a shared public good relied upon by stakeholders worldwide.

The contracting challenges in April 2025 have set the stage for change. Policymakers should embrace this opportunity to thoughtfully and strategically empower cybersecurity practitioners to improve vulnerability management.

This paper proposes one course of action to modernize and expand the CVE Program into a Global Vulnerability Catalog. It provides a framework for national vulnerability management programs, built atop the global program, to flourish. It stresses the importance of an approach that is consistent with multistakeholder norms that have guided the Internet since its inception. Finally, it provides recommendations for action should policymakers agree with the proposed approach.

Even if these recommendations are taken up, there is still work to be done, both for policymakers and the broader CVE community. While this paper describes a concept for national vulnerability management programs, it does not detail specific elements that policymakers should consider in creating or codifying their efforts. The Secure by Design Initiative (SBDI) at IST will continue to explore this aspect of vulnerability management in future publications.

This paper argues that solving governance challenges with the CVE Program is the most important action in this space for policymakers to tackle. However, there are several operational concerns that can—and should—be addressed even as the structure of the program evolves. In consultation with a broad group of stakeholders, the program should begin to expand open-source software vulnerability coverage, increase transparency, and improve CVE infrastructure in parallel with governance workstreams.

Stakeholders raised other policy issues during development of this paper that could prove fruitful for future applied research and policy development. While there are numerous guides and best practices pertaining to cyber incident response, stakeholders pointed out a lack of guides and best practices related to vulnerability handling, both before and after a patch is available. Several commenters also raised concerns about the viability of Common Platform Enumeration (CPE) as a means to uniquely identify products affected by vulnerabilities. These issues deserve treatment in future research.

Finally—and of particular importance to the SBDI—is the critical relationship between the CVE Program and software safety. The CVE Program is foundational to our collective ability to assess and improve the security of software relied on by individuals, businesses, government agencies, and countless other organizations. Without a robust mechanism for collecting, storing, and analyzing vulnerability data, we cannot respond effectively to security defects, identify root causes of cyber incidents, and track patterns over time. Understanding how these incidents actually happen is essential—not only to respond to them, but also to prevent them from occurring in the future. These efforts can help both direct downstream users of software, as well as those impacted indirectly via the complex web of software supply chains. At present, the CVE Program remains the most powerful tool available for tracking and measuring software security defects at scale. However, unless we address the issues outlined in this paper, we will remain overly reliant on undependable technology—an unacceptable risk in an increasingly digital world.

APPENDIX I - CVE Record Lifecycle

The process of creating CVE Records begins with the CVE Numbering Authorities (CNAs). CNAs create CVE Records at cve.org. They generally include basic information about security vulnerabilities, like a plain-language description of the vulnerability, references to external sources (such as advisories or bug trackers), and the name of the CNA.

It's noteworthy that the system accepts CVE Records that are not complete and accurate, despite the value of such records for downstream customers. Fields that require additional quality control include:

- **Affected Vendor/Project:** The software manufacturer, project name, or open-source project.
- **Affected Product Name:** The specific software product that contains the vulnerability.
- **Affected Version Information:** Specific versions that are affected, often specified as versions or version ranges.
- **Problem Type:** Typically a CWE ID (like CWE-79 for cross-site scripting) when the CNA has information about the underlying weakness.
- **Impact description:** May include qualitative descriptions of impact, such as privilege escalation or remote code execution.
- **CVSS scores:** A standardized framework for rating the severity of a vulnerability.

The CNAs are not required to supply these pieces of data in CVE Records at the time of creation, which creates a gap in the record. As a result, downstream customers of CVE Records may not be able to fully use the records for prioritization and remediation.

According to the CVE Program's website,[63] the current CVE Record lifecycle has six steps:

1. **Discover:** A person or organization discovers a new vulnerability.
2. **Report:** Discoverer reports a vulnerability to a CVE Program partner.
3. **Request:** CVE Program partner assigns a CVE Identifier (CVE ID).
4. **Reserve**: The ID is reserved, which is the initial state of a CVE Record.
5. **Submit:** CVE Program partner submits the details.
6. **Publish:** Once the minimum required data elements are included in the CVE Record, it is published to the CVE List by the responsible CNA.

[63] "Process," CVE Program, last accessed October 2025, https://www.cve.org/About/Process.

While accurate, the above list focuses solely on CVE Record creation. A common next step is ingestion by NIST's National Vulnerability Database (NVD), which copies the record from cve.org and adds missing fields such as CPEs,[64] CVSS scores, CWEs, and configuration details. The NVD "enrichment" process is separate from the CVE Program and is often delayed or incomplete.

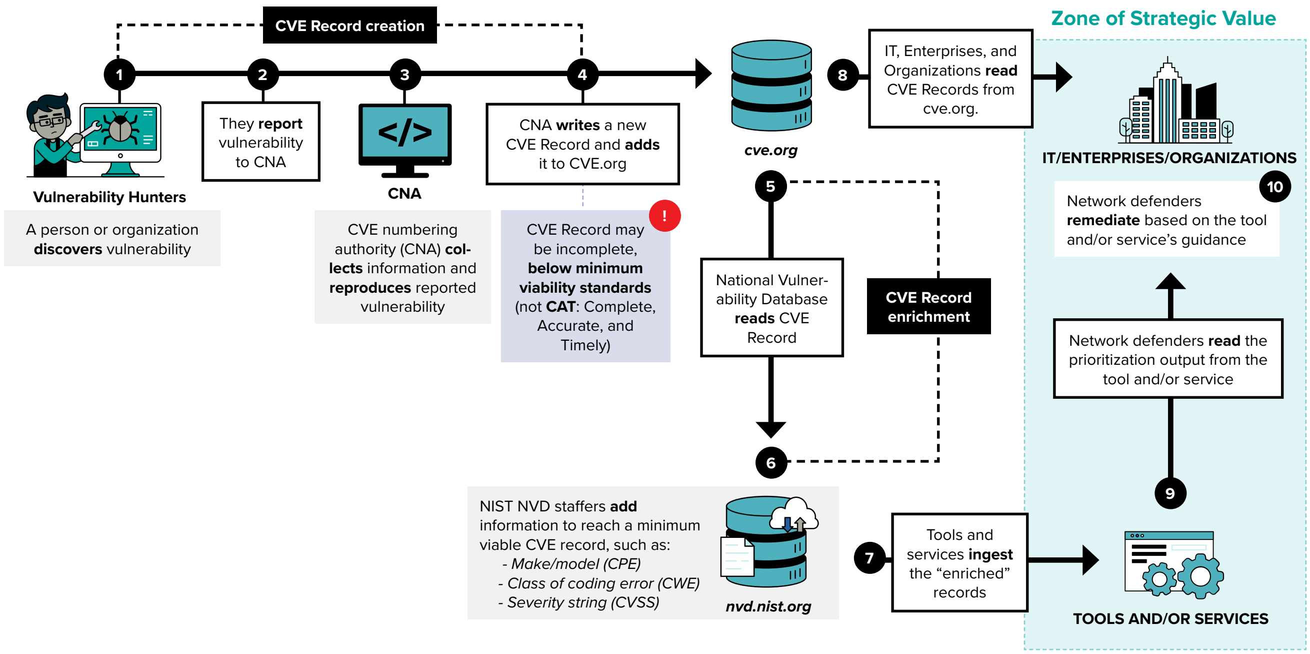
If we adopt a customer-centric mindset, we need to add a few more steps.

7. **Tool intake.** Tools (commercial and open-source) ingest the "enriched" records from NVD. Network defenders in enterprises use these tools to prioritize remediation efforts based on guidance from the tools. Remediations might range from applying software updates, to changing product configurations, or changing network rules to limit access to an affected system.

8. **Data analysis.** To determine the root causes of software security defects, it will be important to track the quality of CVE Records across CNAs, and over time. That analysis can inform changes to the CVE Record schema, the need for particular software manufacturers to focus on certain recurring classes of vulnerability, and even the need for industry-wide solutions for problems that no one entity can resolve on their own.

Here is a simplified view of the current CVE lifecycle:

Figure 1: Current CVE Lifecycle: One Example


CVE Record creation
1
2
3
4
Vulnerability Hunters
A person or organization discovers vulnerability
They report vulnerability to CNA
CNA
CVE numbering authority (CNA) collects information and reproduces reported vulnerability
CNA writes a new CVE Record and adds it to CVE.org
!
CVE Record may be incomplete, below minimum viability standards (not CAT: Complete, Accurate, and Timely)
cve.org
5
National Vulnerability Database reads CVE Record
CVE Record enrichment
6
NIST NVD staffers add information to reach a minimum viable CVE record, such as:
- Make/model (CPE)
- Class of coding error (CWE)
- Severity string (CVSS)
nvd.nist.org
7
Tools and services ingest the "enriched" records
8
IT, Enterprises, and Organizations read CVE Records from cve.org.
Zone of Strategic Value
IT/ENTERPRISES/ORGANIZATIONS
10
Network defenders remediate based on the tool and/or service's guidance
Network defenders read the prioritization output from the tool and/or service
9
TOOLS AND/OR SERVICES

[64] "Official Common Platform Enumeration (CPE) Dictionary," NIST National Vulnerability Database, created September 20, 2022, updated August 20, 2025, https://nvd.nist.gov/products/cpe.

It’s important to understand that NVD “enrichments” occur only within the NVD database and are not pushed back into the CVE.org system. This means that the “enriched” data is available only through NVD’s own interfaces and feeds. As a result, there are effectively two parallel representations of the CVE: the concise and authoritative record at CVE.org, and the enhanced but derivative version at NVD. This separation can create confusion among users who expect CVSS scores or CWE tags to be part of the “official” CVE data, when in fact those fields are entirely owned and maintained by NIST.

Despite historical reasons for this split in roles and responsibilities, it should be clear that the current process flow does not force the creation of CVE Records that are complete, accurate, and timely, and that can be immediately be ingested into vulnerability management tools to help defenders decide how to manage the risks created by software.

The current approach is to allow CNAs to create incomplete CVE Records, and then to have the U.S. federal government attempt to fill in the gaps. This creates the classic problem of trying to fix problems downstream that were created upstream. It’s an approach that suffers from multiple problems, especially around data quality and scalability. Indeed, we’ve seen exactly this problem with a slowdown in NVD processing.

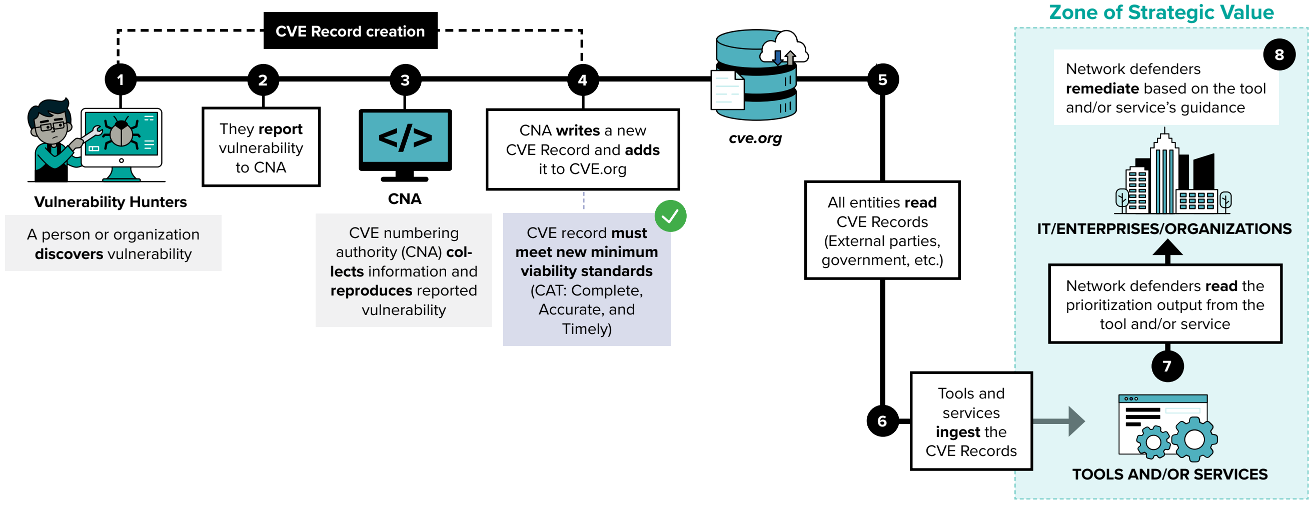
MITRE is charged with the operations of the CVE Program, but the NVD, as part of NIST, is a separate program with separate staff, goals and funding.

A different approach would be to work with the CNA community to increase the minimum viable CVE Record. Such an increase in the minimum viable CVE Record standard would be a minimal change. Commercial software manufacturers and open-source maintainers know the names of their software better than the government does. They are equally better positioned to know the organization that created them, the affected version numbers, and the type of vulnerability.

If CVE Records were created with the minimum viable fields, there would be no need for downstream organizations to “enrich” sub-viable records. If the systems and workflows favored CVE Records that were complete, accurate, and timely, the system would scale with the increase in software and software adoption, and would improve CVE Record quality.

Here is a view of a proposed CVE lifecycle:

Figure 2: Proposed CVE Lifecycle: One Example


CVE Record creation
1
2
3
4
5
6
7
8
Vulnerability Hunters
A person or organization discovers vulnerability
They report vulnerability to CNA
CNA
CVE numbering authority (CNA) collects information and reproduces reported vulnerability
CNA writes a new CVE Record and adds it to CVE.org
CVE record must meet new minimum viability standards (CAT: Complete, Accurate, and Timely)
cve.org
All entities read CVE Records (External parties, government, etc.)
Tools and services ingest the CVE Records
Zone of Strategic Value
Network defenders remediate based on the tool and/or service's guidance
IT/ENTERPRISES/ORGANIZATIONS
Network defenders read the prioritization output from the tool and/or service
TOOLS AND/OR SERVICES

If we were designing the CVE Program from scratch today, we would almost certainly define a higher minimum viable standard for CVE Records than we have today. That standard would make records immediately useful to network defenders, both directly (through the cve.org website) and indirectly (through tools that ingest the records automatically).

A system with fewer moving parts, and with the responsibility for CVE Record quality placed on upstream providers, would be more efficient and effective. It would help highlight products with better security characteristics and make it easier to identify classes of security defect that require a coordinated, industry-wide response rather than improved diligence from individual software providers.

INSTITUTE FOR SECURITY AND TECHNOLOGY

www.securityandtechnology.org

info@securityandtechnology.org