Cybersecurity Tech Accord calls for enhancing the CVE Program to build a more robust global vulnerability redress ecosystem

BRUSSELS, BELGIUM. - To bolster the global cybersecurity framework the Cybersecurity Tech Accord believes it's crucial to recognize the importance of the Common Vulnerabilities and Exposures (CVE) Program and to register our strong support for it. This program is key for identifying, cataloging, and distributing details about security vulnerabilities worldwide which facilitates rapid, coordinated risk management across both public and private sectors. A strong, transparent CVE Program is vital for minimizing exposure to threats and supporting responsible vulnerability disclosure at an international level.

The Need for Stronger International Cooperation

Even though the CVE Program has global significance, its stability and success currently rely heavily on oversight and funding from the United States Government, which has for many years been doing so as a form of global public good for which it deserves the thanks of the global security community. Recent events have exposed that relying upon any one stakeholder for maintenance and resourcing of a critical global resource carries risks that a more broad-based resourcing model would help to prevent. For example, in April 2025 the program funding nearly ended precipitously. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) responded just in time with a contract extension and further financial support and unveiled a forward-looking Vision Paper, demonstrating leadership but the situation did demonstrate that the program is dependent upon a single funder. To give the CVE Program resourcing on a broader base we suggest an approach based upon shared responsibility with active participation from governments more globally.

Taking action together to address vulnerabilities helps minimize cyber incidents by reducing the attack surfaces of systems and reducing the impact of attacks by facilitating more rapid remediation of vulnerabilities. Governments must go beyond simply supporting voluntary standards, they should take real steps to strengthen the vulnerability management system by helping fund the CVE Program, joining its governance, and harmonizing national policies for vulnerability disclosure based upon good practices more generally. This involves providing legal protections for ethical researchers, building cross-border systems for reporting vulnerabilities, and backing the development and

maintenance of a universal CVE database. By becoming more involved, governments can speed up remediation, reduce risks, and foster trust in cybersecurity processes globally.

The Tech Accord urges governments to see the CVE Program as critical digital infrastructure and join its stewardship. Moving forward requires more than passive approval, it calls for proactive investment, policy alignment with global best practices, and ongoing collaboration with industry and civil society. Only through shared commitment can we secure the CVE Program's resilience and effectiveness, strengthening the foundations of global cybersecurity and limiting the risks arising from vulnerabilities in our increasingly connected world.

The CVE Program serves as a backbone of worldwide cybersecurity infrastructure, facilitating risk management in today's complex digital landscape for both public and private users. It offers a standardized, reliable way to identify and disseminate information about cybersecurity vulnerabilities. The April 2025 incident highlighted a pressing need for stable, transparent funding and innovative solutions to improve the CVE Program. It also presented a valuable chance for stakeholders to cooperate and guide the evolution of the CVE Program. By working together with CISA, we can collaborate to fortify the program moving forward.

The Future of the CVE Program

After engaging with the cybersecurity community about the near funding lapse CISA published its CVE Vision Paper on September 10, 2025. The document lays out CISA's main goals for enhancing the CVE Program, focusing on strong governance, transparency, and active community involvement.

In the Vision Paper CISA established the Quality Era Lines of Effort to drive improvements within the CVE Program. CISA sees the CVE Program as an essential public good, stressing impartial management, wide engagement, transparency, and accountability. Their "lines of effort" include:

- Expand Community Partnerships: Broaden the advisory board to better reflect the ecosystem and spur innovation.
- Government Sponsorship: Secure ongoing investment in CVE infrastructure and services, considering varied funding sources.
- Modernization: Fast-track infrastructure upgrades, automation, and service enhancements, including improved CNA support and expanded API functions.
- Transparency and Communication: Provide regular updates, seek feedback, and collaborate with global partners.

- Data Quality Improvements: Monitor and elevate the completeness of CNA contributions, raise standards for CVE record quality, and introduce new tools like Vulnrichment and Authorized Data Publisher (ADP).
- Advancements in CNA of Last Resort (LR): Boost transparency, responsiveness, and data enrichment, with CISA leading these efforts.

The Cybersecurity Tech Accord supports CISA's objectives for the CVE Program and these initiatives. Both are committed to open management, wide community involvement, and ongoing innovation in vulnerability management, reinforcing a cooperative strategy to strengthen global cybersecurity.

Aligning with CISA and Moving Forward Together: Tech Accord Signatories Supporting the CVE Program

The Cybersecurity Tech Accord's aims for the CVE Program match CISA's vision, prioritizing stability, continuity, and innovation. More could be done by designing in specific action metrics, indicators for measurable results, and consistent milestone tracking and publication. This will help turn high-level objectives into practical outcomes and allow everyone to assess progress and more readily identify opportunities to get involved in developing solutions.

Through collaborative efforts by industry, government, and the global security community, the CVE Program can remain resilient, transparent, and innovative. CISA merits recognition for its leadership and openness to change and stakeholder input. With continuous partnership, clear objectives, and actionable recommendations, the CVE Program will continue to underpin global cybersecurity, safeguarding users and organizations around the world.

Now is the time to turn principles into action. Governments need to step up, invest resources, and actively contribute to the future of the CVE Program. In doing so, they'll help create a safer, more reliable digital environment for everyone, fulfilling the promise of a truly global, cooperative model for cybersecurity.