

OWASP announces participation in the US AI Safety Institute Consortium (AISIC)

OWASP, with its two leading projects AI Exchange and Top 10 for LLM Apps, will be one of more than 200 leading AI stakeholders to help advance the development and deployment of safe, trustworthy AI under the new U.S. Government safety institute.



Wilmington, Delaware Feb 15, 2024 ([IssueWire.com](https://www.issuewire.com)) - Today, OWASP announced that its two leading AI projects **the AI Exchange** and **Top Ten for LLM Applications**, have joined together more than 200 leading artificial intelligence (AI) stakeholders to participate in a Department of Commerce initiative to support the development and deployment of trustworthy and safe AI. Established by the Department of Commerce's National Institute of Standards and Technology (NIST), the U.S. AI Safety Institute Consortium (AISIC) will bring together AI creators and users, academics, government and industry researchers, and civil society organizations to meet this mission.

"We are thrilled to join AISIC, a unique collaborative partnership dedicated to advancing AI safety. By joining AISIC, OWASP embarks on a pivotal journey towards secure and ethical AI, blending our deep expertise in AI security and our global network of chapters and experts with AISIC's work to shaping future standards. Together, we are forging a safer AI future," said John Sotiropoulos, leading OWASP's participation in AISIC. Both OWASP AI Exchange and the Top 10 LLM projects have been at the forefront of safeguarding AI and working to build partnerships of standards alignment with organizations ranging from CSA, ISO, MITRE, and NIST to national cybersecurity agencies and AI security vendors.

You can read our announcement blog, which provides more details on work and our vision for our AISIC participation,

at https://owasp.org/blog/2024/02/08/OWASP-joins-NIST-AISIC-launch-announcement_post.html

The consortium includes more than 200 member companies and organizations on the frontlines of developing and using AI systems, as well as the civil society and academic teams that are building the foundational understanding of how AI can and will transform our society. These entities represent the US largest companies and innovative startups; creators of the world's most advanced AI systems and hardware; key members of civil society and the academic community; and representatives of professions with deep engagement in AI's use today. The consortium also includes US state and local

governments, as well as non-profits. The consortium will also work with organizations from like-minded nations that have a key role to play in setting interoperable and effective safety around the world.

The **Open Worldwide Application Security Project (OWASP)** is a non-profit that works to improve the security of software through a global community of tens of thousands of members and 250+ local chapters worldwide. OWASP's mission is "to be the global open community that powers secure software through education, tools, and collaboration". Its Top 10 lists and other materials set the standard in the world of security. Our freedom from commercial pressures allows us to provide unbiased, practical, and cost-effective information about security in a transparent and open way. Almost everyone associated with OWASP is a volunteer, including the OWASP board, chapter leaders, project leaders, and project members. The organization actively supports innovative security research with grants and infrastructure.

Media Contact

OWASP AI Exchange & Top 10 for LLM Applications

john.sotiropoulos@owasp.org

+1 (917) 242-4285

Source : OWASP

[See on IssueWire](#)