Coalition for Secure AI Forms Technical Steering Committee to Advance AI Security Workstreams

J.R. Rao of IBM and Akila Srinivasan of Anthropic Elected to the OASIS Open Project's TSC Leadership

BOSTON, MA, UNITED STATES, October 15, 2024 /EINPresswire.com/ -- The Coalition for Secure AI (CoSAI), an OASIS Open Project, announced the formation of its Technical Steering Committee (TSC), which is responsible for the overall technical health and direction of the project. The TSC will advise the Project Governing Board (PGB), oversee releases, and manage the efforts of the project's three initial workstreams along with their respective chairs, contributors, and maintainers. The TSC will promote initiatives that align with CoSAI's mission to promote secure-by-design AI systems.

J.R. Rao from IBM and Akila Srinivasan from Anthropic have been elected co-chairs of the TSC. They will play a central role in steering the direction of the workstreams to ensure that they contribute to the overall goals of CoSAI. J.R. and Akila bring a wealth of experience and leadership from their respective organizations and will be instrumental in driving CoSAI's technical direction.

"Securing AI, openly and collaboratively, will be critical for inspiring trust and enabling its acceptance by consumers and enterprises alike. As TSC co-chair, I am committed to guiding CoSAI's three workstreams to establish best practices and frameworks that enhance the security of AI systems," said J.R. Rao, TSC co-chair, of IBM.

"As co-chair of the CoSAI TSC, I'm committed to developing frameworks and controls that help us attest to the trustworthiness and integrity of AI models," said Akila Srinivasan of Anthropic. "By fostering transparency and control, we empower organizations to build secure and responsible AI systems that protect users and pave the way for a safe and innovative future."

The TSC has launched three workstreams aimed at advancing the security of AI systems and will

oversee their efforts to establish best practices, governance, and frameworks for AI security:

- Software Supply Chain Security for AI Systems: This workstream focuses on enhancing AI security by addressing the challenges of third-party model risks, provenance, and AI application security. It builds upon widely recognized security frameworks like the SSDF and SLSA, extending them for AI development.

- Preparing Defenders for a Changing Cybersecurity Landscape: Designed to equip defenders with a comprehensive framework, this workstream will focus on identifying necessary security investments to counter emerging AI-driven offensive capabilities.

- AI Risk Governance: This workstream will develop a comprehensive risk and controls taxonomy, checklist, and scorecard for assessing, managing, and monitoring the security of AI systems across industries.

The governance structure for these workstreams ensures community collaboration, transparency, and alignment with CoSAI's long-term goals. For more details on the governance model, visit the TSC and Workstream Governance documentation in GitHub.

About CoSAI:
CoSAI is an open source ecosystem of AI and security experts from industry-leading organizations dedicated to sharing best practices for secure AI deployment and collaborating on AI security research and product development. CoSAI operates under OASIS Open, the international standards and open source consortium.

Media inquiries: communications@oasis-open.org

Carol Geyer
OASIS
+1 941-284-0403
email us here