Center for Internet Security Launches AI Cyber Defense Pilot to Strengthen State and Local Government Cybersecurity

CIS and MS-ISAC collaboration with OpenAI will explore how AI can strengthen the cyber defense, resilience, and threat response of U.S. critical infrastructure

CLIFTON PARK, NY, UNITED STATES, September 4, 2026 /EINPresswire.com/ -- The Center for Internet Security, Inc. (CIS), in collaboration with OpenAI, today announced an AI Cyber Defense Pilot designed to help U.S. State, Local, Tribal, and Territorial (SLTT) governments and critical infrastructure organizations harness the power of artificial intelligence to enhance cybersecurity and resilience.

As cyber threats become more sophisticated and widespread, foreign adversaries continue to target the nation's critical infrastructure. At the same time, many public sector organizations and critical infrastructure operators must defend increasingly complex environments with limited resources.

> At a time when defenders at the state and local government level are challenged by a growing threat landscape, AI has the potential to be a game changer."
> *Brian Calkin, Chief Technology and Innovation Officer at CIS*

The initiative will bring together government and critical infrastructure organizations, including members of the MS-ISAC community, of varying sizes, regions, and cybersecurity maturity levels to examine how AI can be applied to real-world cybersecurity challenges. The pilot program will evaluate AI's potential to help organizations detect risks faster, better prioritize security actions, strengthen cyber hygiene, and improve overall cyber readiness.

"The services Americans rely on every day are increasingly in the crosshairs of cyber threats. At a

time when defenders at the state and local government level are challenged by a growing threat landscape, AI has the potential to be a game changer," said Brian Calkin, Chief Technology and Innovation Officer at CIS. "This pilot will help us understand how AI can help organizations make smarter decisions, respond faster, and focus on the risks that matter most. The lessons we learn can help strengthen cyber resilience for communities across the country."

The effort will be informed by the operational experience and cybersecurity expertise of the MS-ISAC community, which works daily to help SLTT governments prevent, detect, respond to, and recover from cyber incidents. That perspective will help ensure the pilot focuses on real-world challenges facing public sector defenders.

Participating state and local organizations will leverage OpenAI's technology to help identify, validate, and prioritize findings, support remediation efforts, and advance cybersecurity best practices aligned with the CIS Critical Security Controls® and essential cyber hygiene criteria.

"We have a defender's window: a narrowing opportunity to use frontier AI to close security gaps before attackers seize them. Our partnership with CIS and the MS-ISAC is about making sure that opportunity reaches the defenders protecting essential services — including smaller and under-resourced teams — with the tools, training, and support to use AI for stronger defenses," said Sasha Baker, Head of National Security Policy at OpenAI. "What we learn from this pilot can help extend those capabilities to communities across the country, so that Americans everywhere are better protected from emerging cyber threats."

In addition to supporting pilot participants, the initiative will produce implementation guidance, lessons learned, and recommendations to inform future adoption of AI-powered cybersecurity capabilities across the public sector and critical infrastructure community. Together, CIS and OpenAI aim to identify practical, scalable approaches that can help defenders reduce risk, improve resilience, and better protect the essential services Americans rely on every day.

The pilot reflects CIS's broader commitment to helping SLTT government organizations navigate the opportunities and challenges presented by artificial intelligence. As AI becomes increasingly integrated into government and critical infrastructure operations, organizations must balance innovation with a risk-based approach to security, transparency, resilience, and accountability. Through its growing body of AI security resources, research, and best practices, CIS is providing practical guidance on secure AI adoption, governance, and emerging threats, helping organizations build confidence in the responsible use of AI. Additional resources on security artificial intelligence are available at cisecurity.org/topics/securing-artificial-intelligence.

For additional information or media inquiries, please contact CIS Senior Media Relations Manager, Kelly Wyland, at media@cisecurity.org.

###

About CIS:
The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities. To learn more, visit cisecurity.org or follow us on X: @CISecurity.

About MS-ISAC:
The Multi-State Information Sharing and Analysis Center® (MS-ISAC®) is the trusted nationwide network for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) governments. The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's SLTT governments through coordination, collaboration, cooperation, and increased communication. The MS-ISAC is a division of the Center for Internet Security® (CIS®), a 501(c)(3) nonprofit. Visit MS-ISAC or email info@msisac.org for more information.

Kelly Wyland
Center for Internet Security
+1 518-256-6978
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X

This press release can be viewed online at: https://www.einpresswire.com/article/939706056

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.