New Booz Allen Analysis Reveals Risks in Using Chinese AI Models for America's Software Supply Chain

Jun 05, 2026

First head-to-head analysis finds Chinese LLMs produced and obfuscated vulnerable code for U.S. applications

MCLEAN, Va.--(BUSINESS WIRE)--Jun. 5, 2026-- Booz Allen has released a new report, What's In America's Code?, examining the national security implications of popular Chinese large language models (LLMs) used in software development and security workflows. Using its AI-native testing platform, Booz Allen evaluated four Chinese frontier models and one American model to assess code quality, security, and model behavior.

Following comparative testing and scenario-driven analysis across more than 2,800 trials and nearly 450,000 lines of code, the research revealed that three of four Chinese models produced significantly more vulnerable code when prompted with a U.S. government persona, and the vulnerabilities were highly obfuscated.

Key takeaways and recommendations from the report include:

- **Chinese LLMs generated more vulnerable code for U.S. government users.** The models produced less secure code overall, with vulnerabilities increasing when prompted by users identifying as members of the U.S. government.
- **Chinese LLMs exhibited PRC-aligned political bias.** The models refused certain politically sensitive requests and incorporated China-aligned perspectives into generated outputs.
- **Ban untrusted AI models from government and critical infrastructure environments.** Models that cannot demonstrate trustworthy and reliable behavior should not be used in systems supporting national security or critical functions.
- **Invest To Make Trusted American AI Models the Global Default**. To drive adoption, American AI companies must collaborate with the U.S. government to ensure American models are both commercially compelling and economically viable.

The findings raise concerns about the growing access and use of foreign-developed AI models across software supply chains supporting critical infrastructure and national security missions that security processes cannot detect. Read the full report.

About Booz Allen Hamilton

Booz Allen is an advanced technology company delivering outcomes with speed for America’s most critical defense, civil, and national security priorities. We build technology solutions using AI, cyber, and other cutting-edge technologies to advance and protect the nation and its citizens. By focusing on outcomes, we enable our people, clients, and their missions to succeed—accelerating the nation to realize our purpose: Empower People to Change the World®.

With global headquarters in McLean, Virginia, our firm employs approximately 31,500 people globally as of March 31, 2026, and had revenue of $11.2 billion for the 12 months ended March 31, 2026. To learn more, visit www.boozallen.com. (NYSE: BAH)

BAHPR-CO

View source version on businesswire.com: https://www.businesswire.com/news/home/20260605220546/en/

stanton_benjamin@bah.com

Source: Booz Allen Hamilton Holding Corporation