ALERT

House Homeland Security Hearing Highlights Growing Cybersecurity and Critical Infrastructure Risks of AI

By Shruti Bhutani Arora, Brian E. Finch, Nathan D. Banks

TAKEAWAYS

- The hearing underscored that AI governance, cybersecurity, software supply chain risk, critical infrastructure resilience and data privacy are quickly converging into the same policy conversation.
- Companies should assess AI adoption as part of the broader cyber and privacy risk management program, particularly where AI tools are being used to write code, support cybersecurity functions or operate across enterprise systems.
- Policymakers appear increasingly focused on operational questions, including where AI models come from, what systems they can access, how AI-enabled vulnerabilities are identified and remediated, and whether existing safeguards are sufficient to address cyber misuse and surveillance risks.

06.09.26

On June 4, 2026, the House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection held a hearing on "The AI Security Landscape: How Frontier Models, Agentic AI, and AI Coding Tools Are Reshaping Cybersecurity and Critical Infrastructure Resilience." The hearing focused on how advanced AI systems are changing both sides of the cybersecurity equation: giving defenders new tools to identify, prioritize and remediate vulnerabilities, while also giving adversaries the ability to scale vulnerability discovery, exploitation, reconnaissance and malware development.

The hearing occurred shortly after President Trump issued an Executive Order (EO) on AI innovation and cybersecurity. The EO was repeatedly discussed as a key policy backdrop to the hearing. Chairman Andy Ogles (R-TN) emphasized that the order directs federal agencies to develop a classified benchmarking

process for advanced AI cyber capabilities and establish a voluntary framework for early government access to covered frontier models.

The discussion was centered on three overlapping developments: (1) frontier models with advanced cyber capabilities, (2) agentic AI systems that can operate semi-autonomously across digital environments, and (3) AI coding tools that are increasingly writing production code faster than traditional review processes can keep up.

At a high level, the hearing was not about whether AI will affect cybersecurity. Witnesses and members treated that as settled. The more important question was whether companies, critical infrastructure operators, software vendors and government agencies can adapt fast enough to a threat environment where AI can accelerate vulnerability discovery, exploitation, code generation, incident response and surveillance-related data analysis.

The summary below identifies the key takeaways from the hearing, potential policy and rulemaking signals, and the main issue areas for clients developing, deploying or relying on AI-enabled cybersecurity, coding or infrastructure tools.

Salient Insights

- **AI is accelerating both offensive and defensive cyber operations.** Members on both sides of the aisle framed frontier models, agentic AI and AI coding tools as having immediate operational consequences for critical infrastructure resilience. The discussion focused heavily on power, water, hospitals, local governments, financial institutions, software vendors and the federal government's ability to support under-resourced operators.
- **The central concern is speed and scale.** Witnesses repeatedly emphasized that AI is dramatically increasing the discovery and exploitation of known vulnerabilities, such as memory safety issues and other longstanding software flaws. The problem is that AI can introduce, find and exploit those vulnerabilities at volumes and speeds that existing patch management and review processes were not built to handle. This theme came through in the discussion of AI coding tools, frontier models capable of identifying zero-days and agentic systems that can operate across digital environments with limited human direction.
- **The "patch your way out of it" model is under significant pressure.** A recurring point was that traditional vulnerability management is too slow for an AI-enabled threat environment. One cybersecurity professional emphasized that the exploit window is collapsing, and that defenders will need to move toward more continuous exposure management, automated prioritization, machine-speed mitigation and secure-by-design practices.
- **Agentic AI was treated as a distinct risk category.** The hearing repeatedly distinguished ordinary chatbot-style LLM use from agentic systems that can take actions, invoke tools, interact with code repositories or enterprise systems, and operate across networks with limited human oversight.

- **AI coding tools are changing software security governance.** One AI company CEO focused on the fact that AI coding agents are increasingly writing production code faster than traditional human review processes can keep up. Even if AI-generated code is more secure on a per-line basis than human-generated code, the sheer increase in code volume can still increase the number of vulnerabilities introduced into production systems.
- **Secure-by-design themes were central.** The hearing repeatedly emphasized that companies should be focused on preventing entire classes of vulnerabilities, rather than simply identifying and patching individual bugs. This included discussion of memory-safe languages, AI-assisted refactoring of legacy code, security guardrails for coding agents and stronger expectations for software vendors whose products are used by critical infrastructure operators.
- **Open-source software was treated as a critical infrastructure issue.** Witnesses emphasized that open-source software underpins federal systems, critical infrastructure and commercial products, but is often maintained as a public good without the sustained funding or staffing needed to withstand AI-enabled vulnerability discovery. One witness specifically recommended a major federally supported nonprofit initiative to fund maintenance, security-oriented refactors and remediation of critical open-source components.
- **PRC-origin-open-weight models were a major concern.** Chairman Andy Ogles (R-TN-05) and several witnesses focused on the possibility that Chinese open-weight models could become the default foundation for global developers because they are capable, inexpensive and easy to run locally. The concern was not only direct malicious use, but also supply chain dependence, embedded censorship or model behavior, insecure provenance, adversarial distilled capabilities and adoption of PRC-origin models inside American developer environments.
- **Adversarial distillation is becoming a policy issue.** One witness emphasized that distillation can transfer capabilities from a more advanced model to another model without transferring the original safeguards. This was treated as both a national security issue and a model governance issue, particularly if foreign actors can use outputs from U.S. frontier models to accelerate their own models and then release less-guarded versions broadly.
- **The hearing showed bipartisan concern, but different regulatory priorities.** Republicans emphasized AI competition with China, critical infrastructure resilience, open-weight model strategy, the role of CISA under the new EO and avoiding regulations that could slow U.S. innovation. Democrats emphasized civil liberties, surveillance, privacy, mandatory guardrails, state AI laws and whether voluntary federal frameworks are sufficient. Democratic concerns focused on Section 702, the data broker loophole, government use of AI to analyze large data sets, and the risk that classification or proprietary systems could prevent meaningful accountability when AI systems make mistakes.

Potential Rulemaking/Policy Signals

- **The role of CISA will be closely watched.** Chairman Ogles specifically identified CISA's role under the new EO as an oversight priority, especially whether it can convert early model access into practical guidance and remediation support for critical infrastructure.

pillsbury

- **Future policy may focus on frontier model benchmarking and evaluation.** The EO's classified benchmarking process, combined with hearing discussion about saturated cyber benchmarks, suggests continued interest in government-accessible evaluations for advanced cyber capabilities.
- **Information-sharing may be expanded or clarified.** Meserole called for strengthening existing channels and providing clearer antitrust/export-control guidance so the industry can share meaningful information about frontier AI threats, vulnerabilities and distillation risks.
- **Open-source software security may receive renewed legislative attention.** Cable's testimony strongly supported federal funding for large-scale-open-source maintenance and refactoring, as well as passage of the Securing Open Source Software Act.
- **AI coding security may become a procurement and contractor issue.** Cable recommended that Congress enable AI coding in the federal government and among contractors, but require guardrails to prevent entire classes of vulnerabilities at the point of code generation.
- **State AI laws remain a live federalism issue.** Ranking Member Delia Ramirez (D-IL-03) defended state AI laws and warned against federal action that would undermine state-level AI safeguards before Congress has enacted meaningful federal protections.
- **Civil liberties limits may become part of AI cybersecurity debates.** Matthew Guariglia, senior policy analyst for an AI industry forum, delivered testimony that linked AI cybersecurity to surveillance reform, Section 702, the data broker loophole, transparency and limits on government use of general-purpose AI systems.

Conclusion

The hearing underscored that AI governance, cybersecurity, software supply chain risk and data privacy are quickly converging into the same policy conversation. For companies, the practical takeaway is that AI adoption should be assessed as part of the broader cyber and privacy risk management program, particularly where companies are using AI coding tools, AI agents, AI-enabled security products, third-party models, open-weight models, or systems that combine sensitive data access with autonomous or semi-autonomous decision-making. Policymakers appear increasingly focused on operational questions, including what models are being used, where they came from, what systems they can access, what code they are generating, how vulnerabilities are remediated, and whether safeguards are sufficient to prevent both cyber misuse and inappropriate surveillance uses.

At Pillsbury, we are closely monitoring developments in the AI regulatory landscape. Please do not hesitate to contact us with any questions.