COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

Hearing Statement of Cybersecurity & Infrastructure Protection Subcommittee Ranking Member Delia Ramirez (D-IL)

The AI Security Landscape: How Frontier Models, Agentic AI, and AI Coding Tools Are Reshaping Cybersecurity and Critical Infrastructure Resilience

June 4, 2026

Today's hearing about the security concerns raised by artificial intelligence comes at an important moment. Artificial intelligence development is speeding ahead with nearly no standards, rules, or regulations for how powerful AI tools will be responsibly used. It does not seem to be a point of debate that we should do something about that…

The advent of new models - like Anthropic's Mythos - has moved even the President to admit that there are security risks associated with artificial intelligence and that the Federal government has a role in addressing them. But, as you might expect, I take issue with Trump's recent Executive Order on Artificial Intelligence.

Now, I rarely look to the Vatican for policy inspiration. But when Pope Leo publishes a 200-page encyclical calling for AI regulation and warning that data cannot be left in private hands — and that is a more comprehensive AI policy than what's coming out of the White House — well… we should be concerned. In contrast to Trump's EO, Biden's Executive Order on AI noted that AI makes it easier to "extract, re-identify, link, infer, and act on sensitive information about people's identities, locations, habits, and desires." Bottom line: AI makes it easier to surveil you, target you, and violate your rights and privacy.

And Trump's Executive Order is silent on how to mitigate those risks and protect the public's right to privacy. Am I shocked? No. The administration has already demonstrated it will use every tool available to find, track, and deport immigrants and those who defend their rights. In my own district, DHS has used AI-powered facial recognition software and predictive tools to target and intimidate immigrants and rapid responders alike.

And now we are watching AI-powered monitoring systems spread to schools, to public housing, to hospitals — with no transparency about how they work, no ability to challenge them, and no recourse when they're wrong. So, I am clear we cannot settle for unregulated, unaccountable AI. There must be rules, limits, and oversight. We must set standards for AI's responsible use. "Move fast and break things" is not an acceptable innovation strategy when the things being broken are people's lives, rights, privacy, and safety.

Fortunately, states across the country – including my home State of Illinois - are leading the way. Recently, lawmakers in Illinois sent SB 315, the strongest AI bill in the country, to the Governor's desk. Among other things, the bill requires frontier AI developers to have their safety practices audited by a third party – a major and much-needed check on AI companies.

The effort builds on laws already enacted in states like New York and California that require AI labs to provide information about guardrails to ensure the safety of their models and publish reports on safety incidents.

Bottom line, at the federal level, we need to:

1. Enforce the laws we already have — civil rights, privacy, consumer protection.
2. Define clear rules and guardrails with real consequences that companies are statutorily required to abide by. No voluntary pledges.
3. Make companies prove their systems are safe before release — at every step, the burden of proof should be on the companies, not the consumer or the public.

Until the federal government can do that work and demonstrate it will develop AI policies that prioritize the well-being of the people over the profits of AI companies, Congress must not undermine state laws that ensure the responsible use of AI.

I look forward to hearing from our witnesses today. But I want to be honest about what I'm listening for. Not reassurances. Not promises to do better. Not arguments that protecting people will slow down American competitiveness. I want to know what is being done right now to make sure AI technology will not become another instrument of surveillance, exploitation, or control — dressed up in the language of progress and national security.

We have already endured those who would ask us to sacrifice our rights and liberties to secure our safety. We are done with that false choice.

# # #

Media contact