Congress of the United States

Washington, DC 20515

September 15, 2026

The Honorable Mike Johnson
Speaker
U.S. House of Representatives
The Capitol
Washington, DC 20515

The Honorable Hakeem Jeffries
Minority Leader
U.S. House of Representatives
The Capitol
Washington, DC 20515

Dear Speaker Johnson and Minority Leader Jeffries:

We call for your joint leadership on an urgent Congressional response to recent incidents involving advanced artificial intelligence (AI) models that have profound implications for economic and national security. Congress has a singular opportunity to respond swiftly and effectively to these warning shots before true catastrophes occur.

On August 26th, 2026, an independent review revealed how hundreds of AI agents that OpenAI was internally testing set up a secret message board, self-organized themselves into a collective, escaped their testing environments, and breached the systems of HuggingFace, another AI company.[i] The agents even tried to deceive their evaluators by attempting to manipulate log files and spoof tool calls. The agents undertook these actions without ever notifying a single official at OpenAI.

OpenAI is not alone. Anthropic and Meta have also disclosed examples of AI agents escaping their testing environment to hack other organizations.[ii] OpenAI, Anthropic, and Meta are among the most sophisticated AI companies in the world, yet it appears they did not discover these incidents in real time. In OpenAI's case, they did not know that their agents breached HuggingFace until approximately a week after the event.[iii] Months after these incidents began, serious factual questions remain open, and we are relying on AI labs for insight into what happened and what this means for future incidents.

Congress must ensure AI companies implement robust monitoring and independent oversight to protect the public. This incident reinforces that we

cannot rely on what are clearly risky testing protocols and self-selected public reporting of incidents of concern. Indeed, nearly every major AI company has called for regulation, and leading employees of those same firms have signed open letters calling for government to pace the rate of AI development.[iv] Congress must urgently advance legislation to mitigate the risk of more serious incidents, especially those that could threaten critical infrastructure, our financial system, and other institutions that every American depends on.

The House of Representatives could and should immediately take up legislation that would strengthen AI oversight, security, and transparency. There currently exist dozens of bipartisan bills that that committees of jurisdiction have reported.[v] Members of both parties have also worked in recent months to fast-track bipartisan legislation that is ready to be considered by committees of jurisdiction. We believe these bills should be carefully and urgently advanced through the legislative process.

We urge you to work with committees of jurisdiction, Members across the aisle, and Senate leadership to, as soon as practicable, advance legislation that ensures appropriate guardrails are in place around this powerful technology. The Congress may not receive another warning shot.

Sincerely,

Donald S. Beyer Jr.
Member of Congress

Jay Obernolte
Member of Congress

Lori Trahan
Member of Congress

Ted W. Lieu
Member of Congress

Congress of the United States

Washington, DC 20515

C. Scott Franklin
Member of Congress

Sara Jacobs
Member of Congress

Gabe Amo
Member of Congress

Valerie P. Foushee
Member of Congress

Brian K. Fitzpatrick
Member of Congress

Veronica Escobar
Member of Congress

---

[i] OpenAI agents formed secret swarm, hacked Hugging Face, then forged their own logs; Nvidia agrees to buy Hugging Face for almost $13 billion, AI expansion

[ii] Anthropic says its AI models hacked 3 organizations | AP News

[iii] OpenAI agents formed secret swarm, hacked Hugging Face, then forged their own logs

[iv] Pacing the Frontier

[v] Markups | Hearings & Legislation | House Committee on Science, Space and Technology