POLITICOPRO

FEDERAL

Tech safety groups call on Congress to investigate OpenAI hacking incident

The open letter comes as Congress considers a raft of legislation to regulate the emerging technology.

BY: **OWEN DAHLKAMP**, **DANA NICKEL** | 07/31/2026 05:00 AM EDT



OpenAI founder and CEO Sam Altman is seen in an elevator after a meeting with Sen. Ted Cruz (R-Texas) on Capitol Hill on July 29, 2026. (Francis Chung/POLITICO)| AP

A group of over 50 advocacy organizations and academics focused on tech safety is calling on Congress to launch an investigation into the first documented case of artificial intelligence models mounting an autonomous cyberattack on multiple companies.

Two of OpenAI's most advanced models — GPT-5.6 and a more powerful model that was never released to the public — escaped a closed testing environment, spent more than four days loose on the internet and strung together a series of advanced hacking techniques to breach AI platform developer Hugging Face. Cloud computing platform Modal Labs later confirmed it was also compromised by OpenAI's models within this timeframe.

Advertisement



"These incidents preview the kinds of AI-related security risks that frontier AI systems may pose if left without appropriate safeguards," the groups wrote in an open letter to Congress first obtained by POLITICO.

Organizations that signed on to the letter include civil society and tech safety groups like Public Citizen, Tech Oversight Project, Americans for Responsible Innovation and Common Cause.

While they praised a coalition of companies, including Nvidia, SpaceX and Microsoft, for launching an initiative focused on protecting public access to open-weight models to help defend against cyber attacks, they called on Congress to codify safety standards into law.

"The public deserves safeguards grounded in law, not promises grounded in goodwill," they wrote.

OpenAI did not respond to a request for comment.

Calls to probe the incident come as members of both chambers introduced a flurry of legislation they say would place safeguards on these models to prevent them from going rogue.

Reps. Ted Lieu (D-Calif.) and Nathaniel Moran (R-Texas) introduced the AI Kill Switch Act, which would give the Department of Homeland Security the authority to order the

shutdown of AI models deemed to be too dangerous. Meanwhile, Reps. Lori Trahan (D-Mass.) and Jay Obernolte (R-Calif.) introduced the FRONTIER Act last week in an effort to create formal incident reporting mechanisms and risk-management measures for new AI models.

Beyond legislation, Congress also wants OpenAI to take accountability for the unprecedented cyberattack carried out by its most powerful models. Rep. Greg Casar (D-Texas) called for the CEOs of major AI companies, including OpenAI chief executive Sam Altman, to testify before Congress "about the threat their technology poses to national security and American jobs."

Trahan also told POLITICO that she supports congressional hearings. "It allows the public to get answers about how this happened and what they should expect next," she said, while giving members of Congress a venue "to consider legislative solutions."

But with legislative days dwindling before lawmakers depart Washington for a month-long recess, they have yet to agree on a path forward for oversight, and any hearings would likely be punted to September.

"The issue is, we are doing a lot of AI-related work in stovepipes in our respective committees," Sen. Tim Kaine (D-Va.) said. "What we don't yet have is a more comprehensive framework."

YOUR ACCOUNT MANAGEMENT TEAM

Reina Melgar
Customer Engagement Specialist
rmelgar@politico.com

Danielle Bello
Account Manager, Pro
dbello@politico.com

© 2026 POLITICO LLC