



22 September 2026

Tom Duff Gordon
VP and Head of EMEA Policy
OpenAI
[By email]

Dear Tom,

Subject: AI security

I write to invite you to provide oral evidence to the House of Commons Business, Innovation, Science and Trade Committee on Tuesday 13 October, as we conclude our inquiry into the UK's economic strategy for AI.

Trust has emerged as the core issue in our inquiry, both trust in AI security and safety, and trust that workers and businesses will flourish in an AI-powered economy.

AI clearly has enormous potential to transform UK productivity and growth but the warnings of industry leaders and whistleblowers in recent weeks have demonstrated that the UK's public policy framework and international agreements are not yet fit for the future.

In light of this debate, the Committee has convened an urgent hearing on AI security, to consider the following questions:

1. What capabilities do you expect frontier models to acquire over the next two years, and which present the greatest risk of serious harm or loss of control?
2. What specific capability, failed evaluation or safety incident would cause your company to stop training, withhold a model or withdraw one already deployed?
3. Should AI companies be allowed to decide for themselves whether their models are powerful enough to require independent safety testing? Or should pre-release safety testing be legally mandatory?

4. What legal right to access should the UK's AI Security Institute and other independent evaluators have to your models, training data, testing methods and internal safety evidence? Which results should be published?
5. What powers should a regulator have to prevent deployment, require further testing or withdraw a model that has failed, or has not undergone, an adequate safety assessment?
6. Do you accept mandatory reporting of serious safety incidents, including deceptive behaviour, safeguards being circumvented, unauthorised replication and evidence that human control may be failing?
7. Should different rules govern the release of model weights, given that an open-weight model may become impossible to withdraw or control once released, and where guard rails may be easily disabled?
8. Who within your company is personally accountable for a decision to deploy a frontier model? Should developers bear legal liability for foreseeable harm, and what protection should employees receive when reporting safety concerns?
9. What prevents competition between companies - or between countries - from producing a race to the bottom in safety? Which common international requirements should be mandatory?
10. Do you support slowing the development or deployment of frontier models where safety testing, external oversight or regulatory capacity has not kept pace? If not, why not?

I know that you will want to join us. I would therefore be grateful if you would confirm that OpenAI will make an appropriate representative available, by **Tuesday 29 September**. We would be grateful for your written view on these questions before the time we meet.

Yours sincerely,





Rt Hon Liam Byrne MP
Chair of the Business, Innovation, Science and Trade Committee

**Business, Innovation, Science
and Trade Committee**

House of Commons
Palace of Westminster
London, SW1A 0AA

CommonsBTC@parliament.uk

Bluesky: @hoccommittees.parliament.uk
Instagram: ukcommonscommittees
Facebook: UK House of Commons Committees
LinkedIn: House of Commons Committees

Reddit: u/UKCommonsCommittees
X: @HoCcommitteesUK
Youtube: @ukparliament
parliament.uk