



Rt Hon. Kanishka Narayan MP
Minister of State
(Minister for Artificial Intelligence)
Cabinet Office 70 Whitehall, London
SW1A 2AS

Dame Meg Hillier MP
Chair, Treasury Committee
By email: TREASCOM@parliament.uk

7 October 2026

Dear Meg,

Thank you for your letters of 8 September to myself and Henry de Zoete, Director of the AI Security Institute (AIS), and for your continued interest in AI's impact on the financial services industry. We greatly appreciate the Committee's work on AI. The Committee's report on Artificial Intelligence in Financial Services demonstrates the government collaboration needed to realise the benefits of AI for the UK and strengthen our collective resilience. As agreed with your team, I have collated a response to both your letters into a single return.

The cyber threat to the UK is one of our biggest national security concerns, with new technologies, like frontier AI, continuing to make elements of cyber intrusion operations more effective and efficient. In recent weeks, some of the world's leading researchers have issued stark warnings about the future of frontier AI. There is no credible choice between being ambitious about AI and being serious about its risks. We must do both. This technology has the potential to transform our world for the better. We have a responsibility to make sure it does.

I set out answers to the questions in your letter below, which should be read alongside a [Written Ministerial Statement I made on 7 September](#). I hope that, together, these give a comprehensive overview of the Government's position on a fast-moving topic.

The Government Cyber Action Plan

The Government Cyber Action Plan drives a generational uplift in our cyber defences, protecting critical infrastructure and making sure increasingly autonomous systems are deployed safely. The success of the Government Cyber Action Plan depends upon building durable, system-wide resilience through strong baseline security and cyber hygiene, rather than on access to the capabilities of specific frontier models. Access to frontier models complements, rather than substitutes for, wider cyber resilience activity. While early access to new models can be valuable in identifying novel risks and informing

defensive measures, increasing investment in the rapid improvement of cyber resilience is the primary mitigation.

Nevertheless, leveraging the cyber defensive capabilities of both frontier and sub-frontier models is a valuable complement to cyber security fundamentals. A recent collaboration between AISI and the National Cyber Security Centre (NCSC), used frontier AI models to find vulnerabilities in government owned public code and help spot weaknesses early. In early tests, this approach identified over 400 vulnerabilities.

In July, the Government announced our new Cyber Shield programme: a longer-term, national-scale and collaborative approach to AI-enabled cyber defence, working with industry to identify and mitigate cyber risk. The project is still in its early stages, but we are keen to work with both wider government and industry so that people have every opportunity to contribute. However, I would reiterate that whilst AI-enabled vulnerability discovery is a valuable means of understanding the risk, it is not a substitute for cyber security investment in improving the cyber resilience of institutions.

UK financial authorities' access to pre-release frontier models

The Government is determined that the UK leads the way in being the fastest adopter of AI among the G7. That applies equally to using AI for cyber defence. However, the priority for UK financial regulators is to be aware of the overall trend in model capabilities, rather than focus on access to individual frontier models.

The financial sector is a leading sector both in its commitment to improving cyber resilience and its approach to tackling new risks. Its engagement with government and approach to sharing insights to reduce vulnerabilities is exactly what we need as part of the collective response to AI risks and opportunities.

AISI and NCSC work collaboratively with policy holders such as DCMS, HMT and BIST as well as with cyber regulators, passing on insights and supporting efforts to bolster our collective cyber security.

The Government is also committed to working with regulators to boost their capabilities, and departments are now working proactively with them to provide clear strategic direction and support them on their AI capability needs, including on cyber resilience.

Briefing UK financial authorities and future protection

AISI shares and will continue to share relevant findings on risk and capabilities trajectories with key Government partners including HM Treasury and the Bank of England.

NCSC provides threat assessments to help organisations understand potential cyber risks and make informed security decisions. These assessments combine cyber threat intelligence, research on threat actors, and analysis of emerging vulnerabilities to produce actionable insights for service delivery teams and senior leaders. In addition to trusted,

practical guidance equipping organisations to adopt cyber security fundamentals, NCSC has also published advice on supporting the secure adoption of AI for cyber defence, alongside insights from AISI. DCMS and NCSC continue to engage to support institutions on increasing cyber resilience.

There are immediate actions that all critical national infrastructure (including the finance sector) and public sector bodies should take in response to increasing AI cyber capabilities. First, take cyber security seriously at the very top of the organisation by making it a leadership responsibility and implementing all the actions within the Cyber Governance Code of Practice. Second, sign up to NCSC's Early Warning service to receive advanced notice of potential threats. Third, align your organisation's cyber security to the NCSC's Cyber Assessment Framework (a collection of cyber security guidance for organisations that play a vital role in the day-to-day life of the UK) and require Cyber Essentials (the minimum standard of cyber security recommended by the Government for organisations of all sizes) in its supply chains; ensuring the critical services in your organisations and their supply chains are clearly understood and prioritised. Public sector bodies should also prioritise Government Cyber Action Plan delivery so their cyber posture is proportionate to the risks we are now facing.

AISI frontier access

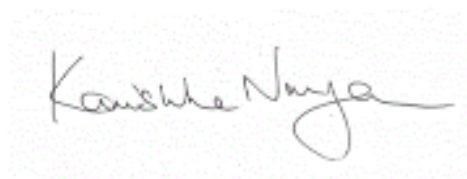
Anthropic made clear at the time of the release of Mythos 5.1 that no organisations outside of the US had access to the model. This does not change the trusted, voluntary relationships that AISI has built with the world's leading AI companies.

AISI is in daily conversation with industry partners, including Anthropic, and maintains long-standing arrangements to test models from major AI developers. Only this month, we tested OpenAI's most powerful model, GPT-6 Astra, before it was released to the public.

Pre-release testing of frontier models is a core part of AISI's work to inform government, but our remit goes beyond that. We have teams of talented AI researchers working on research projects that are fundamental to the UK's understanding of AI risk, across chemical-biological, human influence, and loss of control.

No country can tackle the risks presented by frontier AI alone. AISI frequently and closely collaborates with US counterparts, such as the Center for AI Standards and Innovation (CAISI), to improve the security of new AI models.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'Kanishka Narayan', is centered on the page. The signature is fluid and cursive, with the first name 'Kanishka' being more prominent than the last name 'Narayan'.

**RT HON KANISHKA NARAYAN MP
MINISTER OF STATE (MINISTER FOR ARTIFICIAL INTELLIGENCE)**