Rt Hon Peter Kyle
Secretary of State for Science, Innovation
and Technology
100 Parliament Street
London SW1A 2BQ

E: Secretary.State@dsit.gov.uk
W: www.gov.uk/dsit

Chi Onwurah MP
Chair of the Commons Science, Innovation and Technology
Select Committee

24th February 2025

Dear Chi,

At the Munich Security Conference on Friday 14 February, I announced that the AI Safety Institute would be renamed the AI Security Institute.

This new name better reflects the Institute's focus on serious AI risks with security implications, such as how the technology can be used to develop chemical and biological weapons, to carry out cyber-attacks, and to enable crimes such as fraud and child sexual abuse. Whilst we are optimistic about the extraordinary potential of AI, as reflected in the AI Opportunities Action Plan, we will not be able to seize the opportunity the technology presents unless we mitigate its potential risks.

This change brings us into line with public expectations of an organisation like the Institute. It will not focus on issues such as bias or freedom of speech; those matters are being addressed by my Department through initiatives like the Fairness Innovation Challenge, which supports the development of socio-technical solutions to bias and discrimination, and work on AI assurance, which ensures we're adopting AI safely and responsibly across the economy. Rather, the Institute will focus on advancing our understanding of the most serious risks posed by the technology to build up a scientific basis of evidence which will help policymakers to keep the country safe as AI develops. There has been a clear upward trend in AI system capabilities most relevant to national security in the past 18 months. The more we understand these risks, the better we can work to address them, and to ensure that our people can embrace the potential of AI. A security risk is a security risk, no matter where it comes from. I have therefore instructed the Institute to take a leading role in testing AI models wherever they come from, open or closed. I have also launched a new criminal misuse team in the Security Institute, which will partner directly with the Home Office to conduct research on a range of crime and security issues which threaten to harm our citizens.

The Institute will continue to work closely with partners across government to achieve its objectives. Its team of scientists and experts collaborate closely with the Defence Science and Technology Laboratory, the Ministry of Defence's science and technology organisation to assess the dual-use scientific capabilities of advanced AI. The Institute also works with wider government, the Laboratory for AI Security Research (LASR), and the national security community; including building on the expertise of the National Cyber Security Centre (NCSC), the UK's national technical authority for cyber security, including AI.

Finally, it is important that we do not only focus on the security risks of today, but on tomorrow too. The 2025 International AI Safety Report, led by Yoshua Bengio, warns us that - without the checks and balances of people directing them - we must consider the possibility that risks won't just come from

malicious actors misusing AI models, but from the models themselves. We do not yet know the full extent of these risks, but as we deploy AI across our economy, our society, and the critical infrastructure that keeps our nation secure, we cannot afford to ignore them.

I will continue to update both Houses on the work of the AI Security Institute as it progresses. I will place a copy of my letter in the libraries of both Houses for future reference.

Yours sincerely,

Rt Hon Peter Kyle
Secretary of State for Science, Innovation and Technology