Kanishka Narayan MP
Parliamentary Under Secretary of State
Department for Science, Innovation & Technology
22-26 Whitehall
London SW1A 2EG

www.gov.uk/dsit

Department for Science, Innovation & Technology

15 April 2026

Dame Chi Onwurah MP
Newcastle Upon Tyne
Central and West

Dear Chi,

Thank you for tabling the debate on technology sovereignty on Tuesday 10 March and for your follow-up letter dated Tuesday 31 March.

As you know, the topic of sovereignty is complex and multifaceted. In various settings DSIT and HMG have sought to set out our views and approach, however, I recognise your interest and the critical strategic implications that you place on this topic. Beyond these responses, I would be keen to have a follow-up discussion with you to understand your concerns in more detail and how I can best get your involvement on this topic as it develops. Please find the answers to your questions below.

**1. Big tech and democratic accountability**

The UK does not regard, nor seek to treat, technology companies as sovereign states.

Although some global technology companies operate at significant scale and across multiple jurisdictions, which may require a strategic and coordinated approach, they remain private sector actors and do not possess sovereign authority. Companies operating in the UK are subject to UK laws and regulatory frameworks, which are set by Parliament and enforced by independent regulators.

The Government engages with technology companies, as it does with other major economic actors, to promote growth, innovation, and security, while ensuring that UK interests, democratic accountability, and the rule of law are upheld.

**2. Defining sovereignty and Government position**

The Government has identified the need to strengthen capability across a range of critical technologies, as set out in the Modern Industrial Strategy (2025) and the Digital and Technologies Sector Plan (2025), including building UK capacity in AI computing through investment in advanced compute infrastructure.

In addition, we are exploring - and delivering – a range of additional interventions at all critical parts of the stack. For example, DSIT is launching the Sovereign AI Fund on April 16th to invest in early-stage AI companies with the potential to become global winners in a series of critical AI sectors such as compute & infrastructure, or life sciences and scientific discovery, ensuring they have a stake in Britain. In addition, we are working closely with partners across HMG to ensure we take a full-stack approach (e.g., earlier – such as through ARIA's Scaling Inference Lab for AI Hardware, or later – such as through the British Business Bank's support for AI scale-ups).

In addition, we require the capability to assess and mitigate critical security risks and capability trends as a government itself, which we have through world-leading research and collaborations done by the AI Security Institute.

This Government supports competitive and innovative AI and digital sectors that deliver choice and fair outcomes for UK based businesses and consumers. Strong competition is essential to driving growth, investment and confidence in the UK's digital economy, lowering barriers to entry and ensuring consumers and businesses across the economy are treated fairly.

The Government prioritised the commencement of the digital markets regime in January 2025 and provided a clear steer that these new powers must be used effectively collaboratively and proportionately. In October 2025, the Competition and Markets Authority (the CMA) designated Google with Strategic Market Status (SMS) in general search and search advertising services, and Apple and Google with SMS in mobile ecosystems. Apple and Google have already initiated important commitments from the 1 April in the mobile platform market, while remedies in the search market are expected to be implemented later this year.

More recently, the CMA announced a package of actions in the business software and cloud services market. This includes a new SMS investigation into Microsoft's business software under the new regime. This balanced approach supports competition, growth and innovation while ensuring the digital markets regime delivers real benefits for UK businesses and consumers.

## 3. Cybersecurity, data governance, and foreign dependence

Under UK data protection law, organisations, including government departments, are required to ensure that personal data continues to receive an equivalent level of protection when transferred overseas.

The UK has an adequacy decision for certain transfers to the US under the UK Extension to the EU-US Data Privacy Framework. This decision assessed US laws and practices relating to government access to data, including the US CLOUD Act. This analysis is published and available on GOV.UK. Where adequacy is not relied upon, organisations must use alternative safeguards in line with Article 46 of the UK GDPR, such as standard contractual clauses.

The USA PATRIOT Act does not provide US authorities with unrestricted access to data held by US or UK companies, including those signed up to the Data Privacy Framework. Reforms to US legislation have also strengthened judicial and congressional oversight of such access.

The Government places high importance on protecting the personal data of UK citizens. It continues to monitor both the adequacy decision and developments in US law to ensure that appropriate levels of protection are maintained.

On your question about Cellular information modules (CIMs) - CIMs are widely sourced through global supply chains, and there is no single point of dependence. The Government keeps structural dependencies in critical technology supply chains under review, with a focus on diversification and long-term economic resilience.

Multiple government departments are working closely with international partners to embed resilience into critical UK and global supply chains. This includes:

- Investment screening through the National Security and Investment Act (2021) to manage high-risk suppliers;

- Telecoms and cyber and data security requirements to protect data and networks, including the Telecommunications (Security) Act 2021, the Product Security and Telecommunications Act 2022, and the forthcoming Cyber Security and Resilience Bill.
- Supply chain measures such as the Procurement Act and diversification requirements to reduce dependency and build resilience.

## 4. Open source, procurement, and public sector technology

Individual departments are accountable for applying the Government Functional Standards, including those relating to digital and technology, which have been mandatory since 2021. Compliance is assured through existing departmental governance, assurance and audit processes. There are no current plans to introduce additional centralised public reporting on open standards compliance.

As described in the Roadmap for modern digital government, The Government Digital Service (GDS) is working to publish a National Cloud Strategy in July 2026.

GDS has stood up a team, with responsibility for working with departments, the Government Commercial Function and suppliers to capture data and generate insights on how government technology, including AI-enabled platforms, is procured and where public sector spend is concentrated. The aim of this function is to understand where government services depend on different types of technology suppliers, where we may find efficiencies and where there are risks that need to be managed at a cross-government level.

The Government adopts a balanced approach, seeking to ensure that public sector digital services are secure, resilient and effective, while continuing to benefit from access to the frontier and to global technology markets.

Procurement decisions are taken on the basis of value for money, security and the effective delivery of public services. Decisions affecting critical infrastructure are informed by evidence relating to security, reliability and long-term resilience.

The Sovereign AI Fund will enable government to act as an early customer for a subset of promising AI startups in its investment areas like compute or life sciences (see 2a above), creating the proof points and early revenue they need to attract further private investment.

## 5. International collaboration and sovereignty strategy

We are committed to an open, trusted, interoperable digital future with our like-minded international partners.

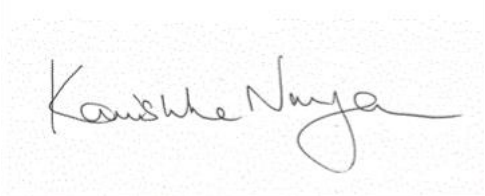
We have partnerships across the world that complement UK capabilities, advance frontier technologies, attract talent and investment, strengthen supply chains, and support UK leadership in global standards and regulation.

Foundational relationships with the US and EU remain central as do our partnerships with countries such as Japan, India, China, South Korea, Switzerland, France, Germany, Brazil and South Africa.

We work closely with the US across strategic technologies as our top research partner and our largest single country trading partner.

As always, I welcome your sustained and constructive interest in this important issue. I hope you found this response useful.

Yours sincerely,



**Kanishka Narayan MP**
**Parliamentary Under Secretary of State at the**
**Department for Science, Innovation &Technology**