Department for Digital, Culture, Media & Sport

Rt Hon Jeremy Wright QC MP
Secretary of State for Digital, Culture, Media and Sport
4th Floor
100 Parliament Street
London SW1A 2BQ

www.gov.uk/dcms
enquiries@culture.gov.uk

Norman Lamb MP
Chair
Science and Technology Committee
House Of Commons
London
SW1A 0AA

TO2019/02263/DC
6 March 2019

Dear Norman,

Security of the UK's Communications Infrastructure

Thank you for your letter of 14 January 2019. I am responding as the Secretary of State with responsibility for telecommunications critical national infrastructure. You raise a number of important questions regarding the security and resilience of the UK's communications infrastructure.

- **How does the government assess and manage the potential national security risk posed by foreign suppliers of telecommunications infrastructure products or services?**
- **How reliant are UK communications networks on foreign-supplied products and services currently?**
- **To what extent can the Government assure the security of the UK's critical communications networks where they are owned and run by private companies?**

Policy responsibility for the security and resilience of the UK telecoms network sits with the Department for Digital, Culture, Media and Sport. However, the international nature of the telecoms market and the sector's vital role in underpinning other critical national infrastructure sectors makes this a cross-government priority. DCMS works closely with the National Cyber Security Centre (NCSC), the Centre for the Protection of National Infrastructure, Ofcom and industry to understand, respond to and address the security and resilience risks faced by the sector.

The global reach of the telecoms market means that our communications companies procure equipment from suppliers across the world. The variety of equipment providers used by UK telecoms companies improves resilience against single points of failure in the network and reduces monopolistic effects in the market. Procurement decisions are made by private companies who provide the UK's telecoms network and are therefore not directed by government. However, companies are required to take appropriate steps to manage risks to the network under existing legislation.

It is important that we and our partners remain confident in the security and resilience of our critical infrastructure, particularly as our networks continue to evolve and given our ambitions to be a world leader in 5G technology and secure the nationwide roll-out of gigabit-capable networks.

The UK, like many countries, is looking at the right policy approach to 5G security. DCMS are leading a cross-government review of the supply arrangements for the UK telecoms sector, working closely with the NCSC and key departments across government. The Review launched in October 2018 and is due to conclude its analysis in the spring. The government will then take decisions. As the public terms of reference[1] make clear, it is a holistic review, taking account of economic, security, quality of service and other factors. It is considering the full range of policy options.

- **What assessment has the Government made of the UK's allies' actions regarding foreign involvement in their communications network, and why has the Government not pursued similar actions in the UK?**

Though the Review will aim to answer a domestic policy question, the telecoms industry is a global market and the Foreign Office is playing a critical role in the Review to actively understand the views and positions of international partners and potential investors. The international reach of our world class network of Posts and trade offices is invaluable to allow the UK to make an informed decision on any future action.

These are complex issues and the global nature of the market, and potential decisions of our partners, only reinforce the need for the Review. Inward investment is crucial for our prosperity and the UK welcomes it. Where national security concerns may arise, for any foreign investment the Government will assess the risks and consider possible responses. So it is right that we should take stock now so that we can make evidence-based decisions to secure our long term national security and the resilience of our telecoms infrastructure.

- **How is the Government responding to the HCSEC Oversight Board's latest annual report?**
- **Does the Government intend to expand the model of the HCSEC to other foreign communications product of service suppliers?**
- **Is the Government considering making the HCSEC mandatory?**

As you are aware, the Huawei Cyber Security Evaluation Centre (HCSEC) operates under a set of arrangements to mitigate any perceived risks arising from the involvement of Huawei in parts of the UK's critical national infrastructure. HCSEC undertakes detailed technical assessments of a range of Huawei products used in the UK telecoms market, with access to information and insight from Huawei which is unavailable to any other facility. These assessments give UK operators and the NCSC evidence to inform commercial and national security risk management. The HCSEC Oversight Board - chaired by Ciaran Martin, CEO of NCSC - oversees and ensures the independence, competence and overall effectiveness of the HCSEC. The Oversight Board's role relates only to products that are relevant to UK national security risk.

---

[1] The Terms of Reference for the Review were published on gov.uk on 8 November 2018, https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference

The HCSEC Oversight Board Annual Report (July 2018) identified technical issues in Huawei's engineering processes. DCMS is represented on the HCSEC Oversight Board and supports the NCSC's continued work with Huawei on its improvement plan to rectify the technical faults identified in last year's report. The Telecoms Supply Chain Review will carefully consider the Oversight Board's findings and conclusions on technical assurance, alongside other evidence, in the development of policy.

- **What assessment has the Government made of the extent to which Chinese legislation could compel Chinese companies active in the UK to assist with Chinese national intelligence work?**

The Chinese National Intelligence Law, passed in June 2017, says that any Chinese individual or organisation can be required by the Chinese state to support, assist or cooperate with national intelligence work. Organisations can also be required to provide access to locations, individuals, and files. Laws of this nature are not uncommon, other nations have them or a relationship between state and intelligence apparatus that does not require a specific law to facilitate unconditional cooperation.

We have serious concerns surrounding the ability of both state and non state actors to gain access to our telecoms critical national infrastructure. As part the Telecoms Supply Chain Review, we are closely examining Huawei's role, and that of other vendors, in our 5G networks and will also take account of the approaches taken by our international partners. The recent attribution of state sponsored malicious cyber activity to the Chinese Ministry of State Security reiterates the importance of our continued vigilance in this area.

We remain, as always, alert and committed to the security of the UK's networks.

I am copying this response to Rt Hon Jeremy Hunt MP Secretary of State for Foreign and Commonwealth Affairs, Rt Hon Gavin Williamson CBE MP Secretary of State for Defence, Ciaran Martin Chief Executive of the National Cyber Security Centre, and Sir Mark Sedwill, National Security Adviser and Cabinet Secretary.

Rt Hon Jeremy Wright QC MP
Secretary of State for Digital, Culture, Media and Sport