Department for
Digital, Culture,
Media & Sport

Rt Hon Nicky Morgan 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

The Rt Hon Norman Lamb MP
Chair
Science and Technology Committee
House of Commons
London
SW1A 0AA

INT2019/09540/DC
6 September 2019

Dear Norman,

Thank you for your letter of 10 July, addressed to my predecessor, regarding the Telecoms Supply Chain Review.

I am grateful to you for writing to outline the findings and recommendations of the Science and Technology Committee's investigation into the telecoms supply chain. The Government considers the security and resilience of our telecoms critical national infrastructure to be of paramount importance, and I am grateful for the work of your committee.

As you know, the Government published the Telecoms Supply Chain Review on 22 July. It outlines the Government's three priorities for the future of telecommunications: (i) stronger cyber security practices among operators; (ii) greater resilience in telecommunications networks; and (iii) diversity in the market. The Review proposes the introduction of a new, robust telecommunications security framework - with new Telecoms Security Requirements (TSRs) at its core - that will meet the security challenges both now and in the future, whilst ensuring the timely rollout of our critical digital infrastructure.

The Review noted that we plan to establish an enhanced legislative and regulatory framework for security, to provide Ofcom with stronger powers to allow for the effective enforcement of the new telecoms security requirements and to establish stronger national security powers for Government. We will also pursue a targeted diversification strategy for the telecoms supply chain over the longer-term.

The Review also looked at how to mitigate the risks from high risk vendors. The Government is still considering its position relating to high risk vendors, following action by the US Department of Commerce which impacted on the review's analysis in this area. Decisions in this area will be made in due course. The Review can be found online at:
https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference

I hope this letter provides a helpful overview of the Government's position on this area. I have also set out responses to the Committee's findings and recommendations in turn below.

- ***"We have found no evidence from our work to suggest that the complete exclusion of Huawei from the UK's telecommunications networks would, from a technical point of view, constitute a proportionate response to the potential security threat posed by foreign suppliers."***

The UK currently uses a risk-based approach to vendors as some vendors pose greater risks than others - this is a fundamental part of our overall mitigation model. As I noted previously, the findings of the Telecoms Supply Chain Review include proposals for a new, more robust telecoms security framework that will raise the bar to meet security challenges now and in the future. The new telecoms security framework will apply to all UK telecoms providers and their suppliers.

- ***"The Government must ensure that it has the measures in place to guarantee that all essential services that make use of communications networks are able to operate safely in the event of network disruption."***

The Government considers the security and resilience of our telecoms networks to be of paramount importance. As risks, threats and technology change it is important that we are able to respond, and that is why we undertook a review of the supply chain to ensure the secure and resilient rollout of 5G and full fibre.

The Communications Act 2003 requires service providers to take appropriate measures to manage risks to the security of public networks and services. The Government therefore expects UK telecoms providers to factor appropriate business continuity and risk management procedures into their operations. The findings of the Supply Chain Review will build on this legislation via the new TSRs, to ensure our new strengthened security framework is sufficient to meet security challenges for now and in the future.

- ***"The Government should mandate the exclusion of Huawei from the core of UK telecommunications networks."***

For the last 10 years, we have had an active mitigation strategy to manage the perceived national security risk of Huawei in the UK's telecommunications networks. We have a deep understanding of Huawei's products and networks, because of our unique arrangement through the Huawei Cyber Security Evaluation Centre and Oversight Board.

The new telecoms security framework proposed in the Review will apply to all UK telecoms providers and through them to suppliers. You will have also been aware that the Review considered how to mitigate risks from high risk vendors. We are still considering our position in this area following action by the US Department of Commerce which impacted on the review's analysis. Decisions on this will be made in due course.

- ***"The Government should monitor Huawei's response to the issues raised by the Huawei Cyber Security Centre's (HCSEC) Oversight Board and be prepared to act to restrict the use of Huawei equipment if progress is unsatisfactory."***

We expect industry to take appropriate account of the advice and guidance issued by NCSC, including the HCSEC Oversight Board Annual Reports. The government will use its membership of the HCSEC Oversight Board to continue to monitor Huawei's response to the findings of successive Oversight Board Annual Reports. The Government will continue to work in close cooperation with industry to ensure the UK's telecommunications systems are appropriately secure and cyber risks are being managed properly, regardless of the vendor used to build the networks.

- ***"The Government should also consult Ofcom on strengthening its powers in order to help improve cyber security in telecommunications networks, and support any changes that are deemed necessary."***

As I previously noted, the Telecoms Supply Chain Review notes that we will establish an enhanced legislative and regulatory framework for security, to provide Ofcom with stronger powers to allow for the effective enforcement of the new telecoms security requirements. The Government and Ofcom are committed to working with telecoms companies to develop the safest and most sensible approach to implementing the new security framework.

- ***"The Government should consult the National Cyber Security Centre on the merit of establishing equivalent cyber security evaluation centres for 5G equipment vendors other than Huawei."***

Government has worked closely with the NCSC throughout the formulation of the Review, and will continue to do so as we work to implement the new security framework for telecoms. We currently adopt a risk-based approach to vendors as some vendors pose greater risks than others, and this is a fundamental part of our overall mitigation model. The new framework will raise the security bar for all vendors, and the new TSRs will require telecoms operators to design and manage their networks to meet the new, strengthened framework.

- ***"The Government must publish the outcome of its Telecoms Supply Chain Review by the end of August 2019."***

The Government published the Telecoms Supply Chain Review on 22 July. We are still considering our position on high risk vendors due to action by the US Department of Commerce which will have implications for telecoms markets globally, and a decision will be made in due course.

Thank you again for your work, and that of your fellow members of the Science and Technology Committee. I am grateful for your continued interest in this area, and I look forward to working with you in the future.

Nicky Morgan

Rt Hon Nicky Morgan MP
Secretary of State for Digital, Culture, Media and Sport