New plans to safeguard country's telecoms network and pave way for fast, reliable and secure connectivity

- High risk vendors to be excluded from sensitive 'core' parts of 5G and gigabit-capable networks
- 35 per cent cap on high risk vendor access to non-sensitive parts of the network
- NCSC issues guidance to operators on implementing decision with legislation introduced at the earliest opportunity

Ministers today determined that UK operators should put in place additional safeguards and exclude high risk vendors from parts of the telecoms network that are critical to security.

High risk vendors are those who pose greater security and resilience risks to UK telecoms networks.

The Prime Minister chaired a meeting of the National Security Council (NSC), where it was agreed that the National Cyber Security Centre (NCSC) should issue guidance to UK Telecoms operators on high risk vendors following the conclusions of the Telecoms Supply Chain Review.

This advice is that high risk vendors should be:

- Excluded from all safety related and safety critical networks in Critical National Infrastructure
- Excluded from security critical 'core' functions, the sensitive part of the network
- Excluded from sensitive geographic locations, such as nuclear sites and military bases
- Limited to a minority presence of no more than 35 per cent in the periphery of the network, known as the access network, which connect devices and equipment to mobile phone masts

As part of the Review, the NCSC carried out a technical and security analysis that offers the most detailed assessment in the world of what is needed to protect the UK's digital infrastructure.

The guidance sets out the practical steps operators should take to implement the government's decision on how to best mitigate the risks of high risk vendors in 5G and gigabit-capable networks.

The government will now seek to legislate at the earliest opportunity to put in place the powers necessary to implement this tough new telecoms security framework.

The government is certain that these measures, taken together, will allow us to mitigate the potential risk posed by the supply chain and to combat the

range of threats, whether cyber criminals, or state sponsored attacks.

The Review also highlighted the need for the UK to improve the diversity in the supply of equipment to telecoms networks.

The government is now developing an ambitious strategy to help diversify the supply chain. This will seek to attract established vendors who are not present in the UK, supporting the emergence of new, disruptive entrants to the supply chain, and promoting the adoption of open, interoperable standards that will reduce barriers to entry.

The recommended cap of 35 per cent will be kept under review to determine whether it should be further reduced as the market diversifies.

Today's decision marks a major change in the UK's approach that will substantially improve the security and resilience of our critical telecoms networks. It will see the government roll out the most stringent set of controls ever – including new standards with tough underpinning legislation to raise the security and quality of the entire 5G and gigabit-capable networks.

Digital Secretary Baroness Morgan said:

> We want world-class connectivity as soon as possible but this must not be at the expense of our national security. High risk vendors never have been and never will be in our most sensitive networks.
>
> The government has reviewed the supply chain for telecoms networks and concluded today it is necessary to have tight restrictions on the presence of high risk vendors.
>
> This is a UK-specific solution for UK-specific reasons and the decision deals with the challenges we face right now.
>
> It not only paves the way for secure and resilient networks, with our sovereignty over data protected, but it also builds on our strategy to develop a diversity of suppliers.
>
> We can now move forward and seize the huge opportunities of 21st century technology.

Ciaran Martin, the Chief Executive of the National Cyber Security Centre, said:

> This package will ensure that the UK has a very strong, practical and technically sound framework for digital security in the years ahead.
>
> The National Cyber Security Centre has issued advice to telecoms

network operators to help with the industry rollout of 5G and full fibre networks in line with the government's objectives.

High risk vendors have never been – and never will be – in our most sensitive networks.

Taken together these measures add up to a very strong framework for digital security.

Further background

The decision today concludes the Telecoms Supply Chain Review, first published in July 2019. The review was a comprehensive, evidence-based review, designed to ensure the security and resilience of the UK's networks.

It recommended new Telecoms Security Requirements (TSR) to provide clarity to the telecoms industry on what is expected in terms of network security.

The TSRs will raise the height of the security bar by setting out to telecoms operators – overseen by Ofcom and the government – the way to design and manage their networks to meet tough new standards.

Another area covered by the Review was how to treat those vendors which pose greater security and resilience risks to UK telecoms.

The Review also highlighted the need for the UK to improve the diversity in the supply of equipment to telecoms networks.

Today the government has announced the final conclusions of the Telecoms Supply Chain Review in relation to high risk vendors. The government, through the National Security Council, asked the NCSC to consider issuing guidance to UK Telecoms operators in relation to high risk vendors. That guidance has been published alongside the final conclusions of the Review.

Notes to editors

Read Baroness Morgan's Written Ministerial Statement to the House of Lords on UK Telecommunications

The NCSC has published a number of documents. These are:

DCMS press office can be contacted on 020 7211 2210.