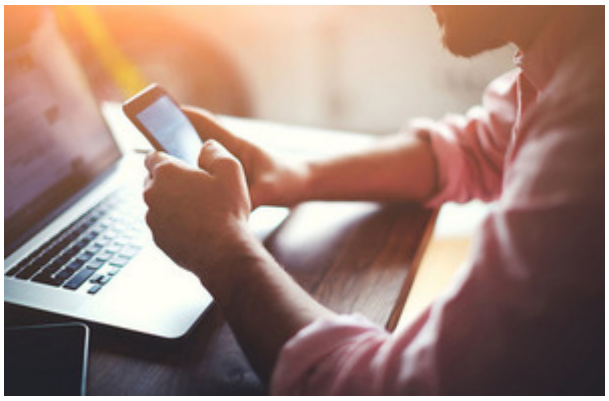
Government plans to safeguard the future security of UK Telecoms

New telecoms security legislation to be introduced and cyber security risks to be prioritised across the sector.

Published 22 July 2019 From: Department for Digital, Culture, Media & Sport, National Cyber Security Centre, and The Rt Hon Jeremy Wright MP



Digital Secretary Jeremy Wright has today set out plans to improve security standards and practices across the UK's telecoms sector, including in new 5G and full fibre broadband networks. The proposals include new legislation to enforce stronger security requirements in the telecoms sector and protect the UK from threats.

The Telecoms Supply Chain Review outlines the Government's ambition to create a sustainable and diverse telecoms supply chain – safeguarding the UK's national security interests and building on our existing capabilities.

At the Supply Chain Review's foundation will be a series of new telecoms security requirements. Overseen by Ofcom and Government, the telecoms operators will need to design and manage their networks to meet these new standards. They will also be subject to rigorous oversight as part of their procurement and contract management processes.

Operators will also need to work much more closely with suppliers to ensure that there is proper assurance testing for equipment, systems and software.

Digital Secretary Jeremy Wright said:

> The UK telecoms sector must prioritise secure and safe networks for consumers and business. With the growth of our digital sector and

> transformative new services over 5G and full fibre broadband in the coming years, this is not something to compromise on. People expect the telecoms sector to be a beacon of safety and this review will make sure that safety and security is at the forefront of future networks.

In response to the Review's findings, the Government will establish a new, robust security framework for the UK telecoms sector – marking a significant shift from the current model.

This new framework will ensure operators build and operate secure and resilient networks, and manage their supply chains accordingly. They will have to assess the risks posed by vendors to network security and resilience, and ensure they manage those risks appropriately.

The Review also identified a lack of diversity in the supply chain and recommends that regulations enforcing telecoms cyber security must be strengthened.

The Government will now develop legislation and look to provide Ofcom with stronger powers. Until then, the government will work with industry to develop new security requirements.

Ciaran Martin, National Cyber Security Centre (NCSC) CEO, said:

> As the UK's lead technical authority, we have worked closely with DCMS on this review, providing comprehensive analysis and cyber security advice. These new measures represent a tougher security regime for our telecoms infrastructure, and will lead to higher standards, much greater resilience and incentives for the sector to take cyber security seriously.
>
> This is a significant overhaul of how we do telecoms security, helping to keep the UK the safest place to live and work online by ensuring that cyber security is embedded into future networks from inception.

High risk vendors

The review also looked at how to mitigate the risks from high risk vendors.

The Government continues to consider its position relating to high risk vendors. Following action by the US Department of Commerce and uncertainty around the implications for the telecoms market as a whole from the entity listing, the government is further considering its position relating to high risk vendors. Decisions in this area will be made in due course.