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

UK TELECOMMUNICATIONS

The Telecoms Supply Chain Review – laid before Parliament in July 2019 – underlined the range and nature of the risks facing our critical digital infrastructure.

The Review addressed three questions:

*How should telecoms operators be incentivised to improve security standards and practices in 5G and full fibre networks? * How should the security challenges posed by high risk vendors be addressed? * How can sustainable diversity in the telecoms supply chain be created?

The Government is establishing one of the strongest regimes for telecoms security in the world. This will raise security standards across the UK's telecoms operators and the vendors that supply them. At the heart of the new regime, will be the National Cyber Security Centre's Telecoms Security Requirements guidance. This will raise the height of the security bar and set out tough new standards to be met in the design and operation of the UK's telecoms networks.

The Government intends to legislate, at the earliest opportunity, to introduce a new comprehensive telecoms security regime – to be overseen by the communications sector regulator, Ofcom, and Government.

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

The Government is developing an ambitious strategy to help diversify the supply chain. This will entail the deployment of all the tools at the Government's disposal. The strategy has three main strands:

- Attracting established vendors who are not currently 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 UK's telecoms operators are leading the world in the adoption of new, innovative approaches to expand the supply chain. The Government will work with industry and like-minded countries to achieve these goals.

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

The Government has now completed its consideration of all the information and analysis on this subject, and is publishing the final conclusions of the Telecoms Supply Chain Review in relation to high risk vendors.

In order to assess a vendor as high risk, the Review recommends a set of objective factors are taken into account. These include:

- the strategic position or scale of the vendor in the UK network;
- the strategic position or scale of the vendor in other telecoms networks, particularly if the vendor is new to the UK market;
- the quality and transparency of the vendor's engineering practices and cyber security controls;
- the vendor's resilience both in technical terms and in relation to the continuity of supply to UK operators;
- the vendor's domestic security laws in the jurisdiction where the vendor is based and the risk of external direction that conflicts with UK law;
- the relationship between the vendor and the vendor's domestic state apparatus; and
- the availability of offensive cyber capability by that domestic state apparatus, or associated actors, that might be used to target UK interests.

To ensure the security of 5G and full fibre networks, it is both necessary and proportionate to place tight restrictions on the presence of any vendors that are identified as higher risk.

For 5G and full fibre networks, the Review concluded that, based on the current position of the UK market, high risk vendors should be:

- Excluded from all safety related and safety critical networks in Critical National Infrastructure;
- Excluded from security critical network functions;
- Limited to a minority presence in other network functions to a cap of up to 35%; and
- Subjected to tight restrictions, including exclusions from sensitive geographic locations.

These new controls will also be contingent on an NCSC-approved risk mitigation strategy for any operator using such a vendor.

The Government intends to bring forward legislation, at the earliest opportunity, to limit and control the presence of high risk vendors in UK networks, and to be able to respond appropriately as technology changes.

Nothing in the Review's conclusions affects this country's ability to share highly sensitive intelligence data over highly secure networks, both within the U.K. and with our partners, including the Five Eyes.

GCHQ have categorically confirmed that how the UK constructs its 5G and full fibre public telecoms networks has nothing to do with how the Government shares classified data.

In response to the Review, the Government has asked the National Cyber

Security Centre to produce guidance for industry in relation to high risk vendors. The guidance sets out how NCSC will determine whether a vendor is high risk, the precise restrictions it advises should be applied to high risk vendors in the UK's 5G and full fibre networks, and what mitigation measures operators should take if using high risk vendors.

The NCSC has published that guidance on their website at: www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks, as well as a summary of the security analysis conducted for the Telecoms Supply Chain Review at: [www.ncsc.gov.uk/report/summary-of-NCSC-security-analysis-for-the-UK-telecoms-sector]. The DCMS press release accompanying this Written Ministerial Statement can be found at: https://www.gov.uk/government/news/new-plans-to-safeguard-countrys-telecoms-network-and-pave-way-for-fast-reliable-and-secure-connectivity.

Copies of these documents have been placed in the House of Commons library.

-END-