Written evidence submitted by techUK (TSB01)

Telecommunications (Security) Bill: Public Bill Committee

techUK

techUK is the trade association which brings together people, companies and organisations to realise the positive outcomes of what digital technology can achieve. With over 800 members (the majority of which are SMEs) across the UK, techUK creates a network for innovation and collaboration across business, government and stakeholders to provide a better future for people, society, the economy and the planet.

techUK is working with our members, telcos, vendors, and regulators on how to continue to improve the security and resilience of our digital infrastructure.

Executive summary

techUK welcomes the opportunity to submit written evidence to the Public Bill Committee on the Telecommunications (Security) Bill. In general, members are supportive of both the intentions and provisions of the Bill, and welcome the clarity provided by the Government on the process for removing High Risk Vendors.

Whilst our members agree with the scope of the Bill as outlined, its inextricable link to the Telecoms Security Requirements (TSRs) means that our submission focuses on both the Bill and the related TSRs and Codes of Practice.

With regards to these Codes of Practice, whilst the Bill applies to all providers, the Codes take a tiered approach based on size and criticality of the provider. To deliver on the Bill's intention it is important that core security duties are applied consistently across these tiers whilst allowing a proportionate approach. Continued engagement with industry is required to ensure that this balance does not result in too complex an approach.

Our submission also outlines where further clarity is required for industry, particularly on the wide-ranging powers given to Ofcom and costs for compliance, security of data in transit, as well as the need for greater transparency. An annex supplements the evidence submitted, which, not directly related to the Bill, aims to provide Committee members with useful material when considering the Bill itself.

Telecoms Security Requirements

Scope

The Bill applies (see Clause 1) to providers of public electronic communication networks/services as defined in the 2003 Communications Act. This means that the subsequent security duties in the Bill will apply to all providers, regardless of size.

This includes providers of communication networks/services to businesses or niche areas of the market who are unlikely to have engaged directly in the process regarding the Telecom Security Requirements to date. The Government has recognised this by differentiating the detail of how a provider would best comply with these duties through a 3-tier system with separate Codes of Practice.

This is essential to ensure proportionality but introduces the additional risk of core security duties not being applied consistently and an overly complex system. Both of these challenges can be overcome but will require continued engagement with the industry on these Codes of Practice.

techUK agrees with the scope of the Bill as outlined but notes that this includes a wide range of providers that are in scope and knock-on impact on the cost of compliance (see below).

Clarity

techUK members are committed to working with Government, Ofcom and the National Cyber Security Centre (NCSC) to ensure the UK's telecommunications networks are secure and resilient. Operators and suppliers working in the UK have long-standing and robust security protocols, maintaining international reputations in multiple telecommunications markets. Communications providers and their partners use stringent security principles in network architectures to protect networks and consumers from hostile acts.

This is not only good practice, but there is a commercial incentive as high-quality security is demanded by customers, especially in business markets. It is also important to note that the current security regulatory requirements have been in force in the UK since May 2011, and the sector is also subject to the General Data Protection Regulation and the E-Privacy Directive.

Much of the concerns that techUK members have stems from the lack of clarity on how the NCSC's Telecoms Security Requirements (TSRs) and Codes of Practice will work in practice. The TSRs themselves are noted to be comprehensive and reflect ongoing security measures operators and service providers already have in place. There is concern that the requirements will be prescriptive, rather than outcomes-based, meaning that they will be difficult for the range of providers (in terms of size and network design) to comply with in a manner appropriate for their business.

Ofcom

The Bill, specifically Clauses 5 to 7, gives Ofcom wide ranging and stronger regulatory powers to monitor, and if required, enforce their security obligations. Greater clarity on Ofcom's role is crucial, including how the regulator sees itself executing its powers in a working regime. The Bill does not specify limitations or thresholds for which Ofcom will enforce the new security framework. It is especially concerning that ongoing compliance assessments under s105N-R do not need to be justified by a suspicion of non-compliance. In order for the regime to workable and targeted, we recommend the introduction of a threshold to ensure proportionality. This threshold should reflect the different Tiers adopted in the Codes of Practice.

The flow of information between operators, Ofcom and the Secretary of State, as a result of Ofcom's powers to issue assessment notices, is also concerning from a commercial and operationally sensitive security perspective, and will increase risk for operators and service providers. The sharing of information with Ofcom, or a third party sanctioned to act as "authorised persons" by Ofcom, will have access to sensitive information and documents. This is a potential significant increase in the number of persons and actors who have access to such information. At the least, we recommend that the characteristics of 'authorised persons' be defined in subsequent Codes of Practice or secondary legislation; including the requirement for Security Clearance where appropriate. We also believe that this flow of information be minimised as much as possible to meet the headline objectives of the Bill.

techUK members also seek clarification on whether Ofcom will have powers to enforce against the TSRs retrospectively. Some members are concerned that under the current TSR framework, some of the provisions are due to be met by mobile network operators in December 2020, despite the Bill not having received Royal Asset.

Codes of Practice

As noted above, in order to ensure proportionality across range of providers that the Bill covers, the Government has proposed a tiered approach to the detailed measures on how best to apply to these duties. Tier 1 providers, which will be subject to the most stringent measures will, according to the impact assessments published alongside the Bill, apply to the largest operators. Tier 2 providers will be for medium sized, regionally important or operators of Critical National Infrastructure, with all other providers being Tier 3.

The same impact assessment makes clear that the cost of compliance will, understandably and rightly, vary by classification of Tier. Government estimates that there will be between 10-20 Tier 1 providers with a far larger number of Tier 2 and 3 providers[1]. Whilst techUK agrees with this broad approach there is still uncertainty about which individual providers will be in which Tier and the costs associated with this.

Further clarity is therefore needed on how these will be tiered proportionately, specifically how Government will engage with the market on determining their implementation. Particular consideration needs to be made for UK operators with corporate headquarters outside of the UK operating in the UK, and how to mitigate the risk of an international fragmentation with other security regimes. Security requirements that require country-specific plans or, worse, staff and equipment to be located in-country are impractical and can significantly increase cost and burden.

Clarification is also required on how the Codes of Practice will affect the entire telecommunications supply chain, including other technologies that support communications networks, and which assets within the network architecture is within scope of the Codes of Practice.

Data in transit

With regards to the specific security requirements, the overarching security requirements set out in Clause 1 are well crafted and align to the well-established information security concept of confidentiality, integrity, availability, non-repudiation and authentication (CIANA). Nonetheless, there is an area that requires further clarification. Clause 1(2)(2)(a) to Clause 1(2)(2)(e) concern the security requirements of the signals conveyed by the network and the service itself, and Clause 1(2)(2)(e) and

[1] There are 119 Providers of Electronic Communication Networks/Services who pay administration fees to Ofcom who have an annual turnover of at least £5m. However, there is a far longer tail of up to 8000 micro and small businesses who are classified as Telecoms businesses by the ONS.

Clause 1(2)(2)(f) concern the data at rest (i.e. data stored by electronic means). However, Clause 1 does not appear to cover the security of data in transit; this is of equal importance and would ensure that data moving through a network is adequately secured, namely between the user and the service, and between the service and another service.

A useful point of reference is the set of 5G Security recommendations published by ENISA on 10 December 2020: "5G Supplement - to the Guideline on Security Measures under the EECC[2]"https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc. For example, the guidance stresses the need to ensure real-time network visibility, particularly related to mutli-access edge computing (MEC) that will be prevalent in 5G (see section 4.3). This visibility relates to data in transit- it is important to have visibility of threats traversing the networks so that threats can be stopped in real time.

Such discussions on the technical security requirements (whether they fall under the secondary legislation or Codes of Practice) prove that the devil is in the detail, and it is therefore crucial that Government engages in meaningful and transparent engagement in advance of the regulations being finalised.

Transparency

techUK members are concerned that there has been no public consultation with Government before the Bill, and that there is no planned consultation until secondary legislation. Industry engagement has been patchy and inconsistent to date, particularly with those providers who are outside of the likely Tier 1 providers. Given that the TSRs and Codes of Practice are likely to be extensive, we encourage greater engagement with *all* of industry through appropriate and open means.

Costs

As noted above, the UK's telecoms networks already adhere to and globally are seen to be best-in-class cyber security practices. Despite this the implementation of the TSRs will require significant changes to company operations, training (including on compliance) and processes. Government must recognise that sufficient time needs to be provided to ensure compliance with the TSRs in a proportionate timetable. The Government's Impact Assessment has not been able to estimate these costs in total. However, the familiarisation and oversight costs alone, a small proportion of likely overall costs, for Tier One operators are likely be in the region of £10m in one-off costs.

Telecoms operators will also incur costs for delivering against the TSRs and the costs associated with removing HRVs – estimated by Government to be in the region of £1.7bn, a figure that many techUK members is an underestimate. This figure is also based on the 2027 deadline which means operators can avoid significant service outages, as the removal falls of HRV equipment falls within the cycle of replacing the underlying 4G equipment.

Given the costs of compliance and removal of HRVs, techUK believes that industry should not be required to fund the enforcement regime for example, the assessments of ongoing compliance foreseen under s105N). Rather Ofcom should be funded to undertake this work by the Government. As we note below, whilst we strongly support the efforts to improve security, we must also ensure that we roll out 5G networks to help drive a levelled-up economic recovery.

[2] https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc

High risk vendors

The announcement in July 2020 that required Huawei equipment to be completely removed from the UK's 5G networks by 2027, with a no new buy rule from 31 December 2020, was followed by the setting out of a new hard deadline for the installation of Huawei equipment. Illustrative directions were outlined by Rt Hon Oliver Dowden MP, Secretary of State for Digital, Culture, Media and Sport, during the Bill's Second Reading on 30 November 2020, that made clear Huawei equipment must not be installed in UK networks from the end of September 2021.

techUK members accept the announcement on the removal of high risk vendors by 2027, and welcome the clear direction set out by Government. This clarity, and certainty, has enabled network operators to plan their installation plans and upgrades accordingly.

The technical, commercial and logistical complexity of making changes on this scale to telecoms networks, whilst still providing crucial communication services, should not be underestimated. It is therefore crucial that the 2027 deadline does not change.

The Committee should consider the significant changes operators will need to undertake to meet this deadline.
techUK members emphasise the need for the Government to give long lead times to industry so that alternative suppliers and sub-suppliers can be evaluated, this will help products and services provided not being unduly impacted.

Annex

Diversification Strategy

techUK views the TSB and the Government's Diversification Strategy as closely intertwined, particularly as Ian Levy, NCSC's Technical Director has stated that "we need to diversify the market significantly in the UK so that we have a more robust supply base to enable the long term security of the UK networks"[3]. Whilst the Diversification Strategy is not part of the Bill, we believe that it is of material interest to the Committee.

techUK supports the Government's Diversification Strategy, published alongside the Bill on 30 November 2020, as part of the wider recognition by Government that it must help create sustainable diversity in the telecoms supply chain. We also welcomed the £250 million funding to assist in implementing this Strategy; facilitating support for incumbent suppliers, attracting new suppliers to the UK and the development of open interfaces and standards. Mobile network operators also need to be incentivised to move towards new mobile network architectures, such as disaggregated networks and Open RAN, which will help attract low-risk vendors to the UK market, and encourage smaller players.

However, further ambition is needed in Government's plans to develop domestic capability and establish the UK as a leader in open and disaggregated network architecture. A supportive policy environment is crucial: alongside further funding for R&D in wider telecommunications technology (not solely focused on 5G) there needs to be support for the production of products and delivery of services which is not a direct cost to Government but contributes gross value added (revenue, tax, VAT, jobs and investment).

Understandably, the Government has focused on short-medium term issues in the Strategy. But if we are to capture the economic and innovation opportunities that could be afforded to us by being a global leader in disaggregated networks, we must take action in short order. Of particular importance is the need for a series of testing environments to lower the cost of innovation in this area.

On this point, techUK's understanding is that the National Telecoms Lab, which members support, will drive forward security, performance and resilience testing of new suppliers and technologies against the TSRs before live deployments (i.e. it will operate at Technology Readiness Levels 8-9). The Lab will also support telecoms security research and development through testing new technologies that may present new threats, to which NCSC will have knowledge of. It is vital that the Lab is located within a wider holistic ecosystem adequately, working closely with SmartRAN Open Network Interoperability Centre (SONIC), NEC - NeutrORAN Trial, as well as universities and regional advanced technology hubs to capture the innovation for future networks. This will allow the National Telecoms Lab to remain focused on security and resilience whilst facilitating greater innovation at lower technology readiness levels as part of an ecosystem.

Government should also set out its plans to bolster and upskill the UK's telecoms workforce, and specific plans to get suppliers beyond the research phase to deployment and commercial scaling up of technologies and hardware.

[3] https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk

5G and gigabit broadband are essential drivers of a levelled-up economic recovery

Next generation digital infrastructure like full fibre and 5G form the digital fabric of the next industrial revolution. They are essential technologies if we are to supercharge our economy as we leave the EU and recover from the pandemic. Next generation connectivity is also an important component in levelling up all regions in the UK, building back greener and transforming public services.

The government has set ambitious targets for gigabit-capably broadband coverage by 2025 and for the majority of the population to have 5G services by 2027. These are ambitious infrastructure projects with the vast majority of the capital being invested by the private sector.

Barclays Bank has stated that 5G could supercharge the economy by £15.7bn by 2025. This growth is well spread across the country with increased business revenue of £1.4bn in The North West and £1.3bn in the East of England.[4]

The welcome focus on telecoms diversification by the UK Government has the potential to create new business and jobs, and the opening up of new markets.

21 December 2020

[4] https://www.barclayscorporate.com/content/dam/barclayscorporate-com/documents/insights/innovation/5g-a-transformative-technology.pdf