ISPA response: 'Ensuring access to 'safe' technology: the UK's 5G and national security inquiry'

About ISPA

1. The Internet Services Providers' Association (ISPA) welcomes the opportunity to submit written evidence to the Joint Committee on the National Security Strategy's inquiry on ensuring access to 'safe technology'.

2. ISPA is the trade association for providers of internet services in the UK. ISPA has approximately 150 members, 90% of which are SMEs as well as large multinational companies. We are proud to be an organisation which covers the whole Internet value chain, including companies that provide access, hosting and other online services. We represent the full ecosystem including communications providers that serve consumers and businesses, those that build their own networks and those that resell services via the fixed and wireless networks.

Summary of main points

3. ISPA's main points in the response can be summarised as follows:
   - The most effective way for Government to support the UK telecoms industry is through a consistent, stable and proportionate regulatory framework.
   - Government can further help the sector by continuing its focus on addressing the cyber security skills gap and raising the public's awareness of cyber security.
   - A diverse supply chain has helped enable innovation and competition in the sector, efforts to intervene in the market need to be evidence-based and seek an appropriate balance between security and investment.
   - UK security requirements that go above and beyond other like-minded nations risks increasing barriers to entry for suppliers and decreasing the negotiating power of providers and impacting on innovation.
   - Government and regulators should seek to coordinate advice and standards in a single place to ensure effective implementation of policy and to reduce the burden on ISPs.
   - The Government should seek to respect global norms as far as possible and following Brexit, the UK should seek to ensure standards remain compatible with those in place in the EU and similar countries.

Government support for the UK telecoms industry

4. The UK telecoms industry is commercially-driven and privately-owned with investment to improve infrastructure and services coming from private means rather than public funds. The most effective way for Government to support the UK telecoms industry is through a consistent, stable and proportionate regulatory framework. New, complex regulation across the supply chain that could involve Government retrofitting policy on existing telecoms infrastructure has the potential to undermine this.

5. In addition to a stable environment for investment, Government plays an important role in providing support and guidance to industry and the public. ISPA welcomes the many positive achievements under the current National Cyber Security Strategy (NCSS), particularly the creation of the National

Cyber Security Centre (NCSC) as a valuable authority and resource for industry. ISPA has encouraged members to engage with specific initiatives such as Active Cyber Defence and facilitate discussions. The successes of the previous Strategy must be consolidated and built on through a new NCSS to be put forward as soon as possible.

6. Further support for the telecoms industry is needed in the form of investment in digital and engineering skills and equipping ISPs to compete for global talent to fill the ever-increasing skills gap. Secure infrastructure relies on a workforce with the right mix of skills for its design, implementation and day-to-day operation and development. A recent study commissioned by DCMS found that more than half of all businesses and charities in the UK have a basic cyber security skills gap, with 66% struggling to keep cyber security experts within their companies. It is important that Government action to address the skills gap is clear and measurable, and we await the full DCMS cyber security skills strategy with interest.

7. In addition, the Government should ensure it places an emphasis on raising the awareness of citizens, as well as the public and private sectors, on how to reduce their cyber security risk. Government support has also been key in ensuring that the UK has been a major beneficiary of and contributor to global technology and business innovation. The UK's continued progress relies upon continued Government support in this area. It will enable international partnerships to develop and ensure access to the best technology and skills, whilst maintaining the confidence of the UK Government, citizens, customers and businesses that our digital infrastructure remains safe and secure as cyber threats continue to grow in volume and sophistication. A well-functioning international supply chain for the telecoms sector is vital to support the UK's digital infrastructure needs.

Diversity of supply chain

8. The telecoms sector is a crucial component of the UK economy with advancements in technology and infrastructure underpinning and strengthening many other industries and enabling the UK to continue to be a world leading digital economy. Such advancements are necessary to meet the Government's ambitious targets for gigabit-capable broadband and 5G. The UK currently enjoys a strong and diverse set of network operators and service providers that offer fast, reliable and secure services. A competitive and diverse supply chain helps operators to innovate, achieve efficiencies and ultimately improve the rollout of communications infrastructure.

9. The telecommunications supply chain is global, highly specialised and has been subject to recent consolidation. This has led to a situation where there are a limited number of companies with the scale, expertise and experience to meet the requirements of operators, and offer services on the scale required by to integrate effectively into the global communications network. Whilst Government's stated policy to stimulate diversity in the marketplace is a laudable aim, it is not without challenges. Plans to intervene more to address a perceived market failure must be fully thought through, with a clear policy outcome in mind, to be successful.

10. Although the global market is characterised by a relatively small number of large players who have relative strengths in different areas, there is not one dominant supplier. UK companies typically

adopt a multi-vendor strategy to ensure they are not wholly reliant on a single supplier in the core and access network. This approach, coupled with consistent and robust procurement policies based on a range of criteria, means that multiple suppliers will continue to have the capability to deliver against the UK's network requirements.

11. Security is an important priority for both Government and telecoms providers as it is crucial to maintaining a strong reputation and in delivering fast and reliable services. However, the desire for increased security through potentially restricting access to certain suppliers should be balanced against the importance of maintaining diversity in the supply chain that has helped enable innovation and competition. In fact, additional UK requirements that go above and beyond other nation states risks increasing barriers to entry for suppliers and decreasing the negotiating power of providers to ensure their supply chain take robust security measures. If the Government were to place significant restrictions on foreign suppliers, this would narrow the market even further, and could have a negative impact on innovation.

Policy-making

12. The resilience and reliability of UK networks is of paramount importance to the whole industry. Continued coordination and a balanced, risk-based approach across industry, Government and regulators can help to ensure this. ISPA would therefore stress that any future Government policy is drafted on the basis of strong evidence, particularly with more high-risk suppliers. Policymakers should consider the costs and benefits of any decisions, maintaining a strong focus on the impact policy may have on the economy, in addition to security considerations.

13. It is vital that any policy is proportionate, acknowledging the fact that the risk level for different service providers and customers varies. Effective policy in this area will be flexible, rather than prescriptive; ensuring that requirements are sufficiently nimble in order to keep pace with developments.

14. The UK must be mindful of the complex wider EU legal and policy landscape. In line with this, the UK should seek to minimise the potential for overlapping requirements given the various horizontal and sector-specific policies already in place or soon to be implemented, such as: Articles 40 and 41 of the new European Electronic Communications Code, GDPR, e-Privacy Regulations and the Cyber Security Act's future certifications.

15. There is a complex network of Government departments and agencies involved in the creation and implementation of cyber security policy. This means that new guidance and evolving requirements are regularly published by many different organisations. As new regulations are introduced on top of existing requirements, the legislative and regulatory frameworks governing cyber security policy in the UK become ever more complicated to navigate.

16. The DCMS Supply Chain Review, as part of its initial conclusions published in July, has proposed new Telecoms Security Requirements (TSRs), which will be underpinned by "a robust legislative framework" and that this "new framework is necessary to safeguard the UK's national security

interests". We await further details of the TSRs and would encourage the Government to ensure that any new security requirements are consistent with those currently in place and fully consult with industry. We would therefore recommend that telecommunications national security measures should be channelled via TSRs to minimise reporting requirements and the regulatory burden on operators' security teams.

17. In this context, ISPs of all sizes can find navigating cyber security frameworks a challenge; however, smaller ISPs can find keeping up to date on developments in cyber security policy to be a burdensome full-time job. Without care, this complexity could serve as a barrier to entry to the market, dissuading new entrants and frustrating Government ambitions to foster competition. The Government and regulators should seek to coordinate advice and standards in a single place to ensure effective implementation of policy and to reduce the burden on ISPs.

International cooperation

18. Given that many companies in this sector are global, difficulties will emerge if new standards are established where there are similar standards already in place in other countries. Additional barriers put in place by the UK, beyond those in place in other countries, would negatively affect the diversity of the supply chain.

19. When setting standards, the Government should seek to respect global norms as far as possible. In particular, following Brexit, the UK should seek to ensure standards remain compatible with those in place in the EU in order to maximise the base of compliant suppliers and that such certifications and standards are industry-led, market driven and voluntary. Cyber security is, by its nature, an international issue and this should inform Government thinking on policy in this area.

20. The UK should seek to collaborate with allies and partners in addressing security issues, taking a lead in facilitating constructive dialogue about 5G infrastructure and national security. This work should seek to draw on industry expertise particularly that of ISPs given they are the authorities on the running and management of their networks. In line with this, ahead of contributing to policy discussions, or drafting policy, the UK should consult widely with all relevant stakeholders and conduct full impact assessments identifying the economic, environmental and innovation impacts of planned measures.

21. It is important that the Government feeds back international developments to UK firms to ensure the UK telecoms industry is well informed and has the necessary information to make strategic and long-term decisions.

22. The UK also has influence on suppliers via international standards-setting forums which are key to these global technologies, with Government and a number of UK companies actively represented, this ability for the UK to influence the development of new technology and products through the standards should be maximised and supported by Government.

Conclusion

23. The relationship between the UK's 5G infrastructure and national security is complex and ISPA welcomes the Committee's exploration of this important issue.

24. As highlighted above, this is an intricate policy area in which even small changes to standards and regulations can have a significant impact on telecoms market and the wider economy. Given this, policy must be proportionate, flexible and evidence-based.

25. In order to deliver the twin aims of improving security and encouraging innovation in the telecoms sector, it will be important for the Government to ensure continued diversity in the supply chain, cooperate with international allies and partners, maintain UK influence and inputs to international standards bodies and ensure industry is equipped with the guidance and can access the skills it needs to flourish.