

Security Consultation team  
Ofcom  
Riverside House  
2A Southwark Bridge Road  
London SE1 9HA

Email: [securityconsultation@ofcom.org.uk](mailto:securityconsultation@ofcom.org.uk)

31 May 2022

Dear Ofcom,

### **General policy on ensuring compliance with security duties**

I am writing to you on behalf of Open Fibre Networks Limited (OFNL), part of the BUUK Infrastructure Group of companies, in response to the Ofcom consultation regarding its “General policy on ensuring compliance with security duties” which was published in March 2022. I can confirm that this response is not confidential.

OFNL has been providing gigabit ready full fibre broadband connections to the new build housing sector since 2008 and our fibre networks are often chosen by developers in preference to the solutions offered by the monopoly incumbent. We also operate a wholesale business, Open Fibre Networks (Wholesale) Limited (OFN(W)L), offering wholesale services to Communication Providers across the UK.

### **OFNL views on the proposed Ofcom approach**

Within the context of the increased value that is now attached to technological connectivity, and the mounting threats of cyber-attack, we acknowledge the importance of establishing targeted provisions to ensure the security of our telecommunications networks and services. We therefore fully support the overarching intent of the proposed new regulations and Code of Practice which seek to effectively implement the 2021 Telecommunications (Security) Act.

We also welcome the proportionate approach that Ofcom proposes to take to enforcement, including the clarification provided in Annex 5 which specifically sets out that “the Code [of practice] does not apply to any Tier 3 providers”. An approach such as this recognises that smaller operators pose a far lower risk to the overall connectivity of the communications network than their larger counterparts and prioritises regulatory focus accordingly. It also acknowledges the relative capacity of the respective participants to manage / absorb costs associated with a regulatory investigation or associated penalties. If this type of cost were faced by smaller players in the market, it could materially impact their growth and, in some cases, cause them to exit the market; either of which could negatively impact market growth.

However, there is one area of the proposals where we have an outstanding concern. We would welcome clarification from Ofcom on the way it intends to apply these provisions or, alternatively, would encourage Ofcom to consider a slight modification of its approach.

### **An area of outstanding concern**

Annex 6 of the consultation sets out that the “guidance applies to all providers of Public Electronic Communications Networks (PECN) and Public Electronic Communications Services (PECS)” and goes on to specify that:

“While...the majority of the provisions in the Regulations, and the associated measures in the Code of Practice, address risks that would generally be considered to fall into the category of “cyber security”, some of the provisions and measures are also relevant to ensuring the resilience of networks and services, in particular, regulations 3, 6, 7, 9, 10, 11, 12, 13, 14 and 15.

The combination of these statements suggests that although most of the provisions in the regulations and code of practice will not apply to Tier three providers, certain elements of the regulations referenced in the excerpt above will be applicable to these entities.

We think Ofcom should slightly amend its proposed approach in this area. While we agree that Tier three providers should seek to comply with ‘best practice’ regulations, we note that if they are subject to enforcement action or penalties, this could materially impact their operations and, in turn, restrict the development of evolving market competition. We also note that Tier three will likely comprise a disparate group of organisations, with significant variation in terms of their scale, composition, and scope for growth.

Although we generally agreed with the DCMS proposals set out in its related consultation on [Telecoms security: proposal for new regulations and code of practice](#), particularly those related to tiering, in our response we proposed that DCMS should consider the potential to establish a ‘small operator’ tier. In this respect, recognising the diversity within tier three, we set out that the inclusion of an additional tier would help to better reflect the risk that smaller operators would pose to the market in terms of maintaining connectivity. As such, we suggested that this fourth tier would help to cater for small but growing telecoms businesses and effectively replicate, on the supply side, the protections that are often provided to small and medium enterprises on the demand side.

We do not think that the provisions applicable to entities within the proposed fourth tier would need to be materially different to those applicable to Tier three entities, but the addition of this tier could allow for an exemption to be provided to smaller companies in terms of potential enforcement action or the imposition of penalties. Where these types of arrangements were established, Ofcom would have scope to focus its efforts on resolving these instances of non-compliance, rather than initiating enforcement activity or seeking to implement associated penalties. Where Ofcom provided clarity to market participants (either formally or informally) of its intent to take a targeted / proportionate approach such as this, it would foster investor confidence amongst smaller market participants and potential new entrants as well as providing regulatory certainty with respect to the environment in which

they will be operating. And these would be valuable outcomes given the volume of investment that will be required in the sector in the coming years.

[REDACTED]

Yours sincerely



Keith Hutton  
**Group Regulation Director, BUUK**