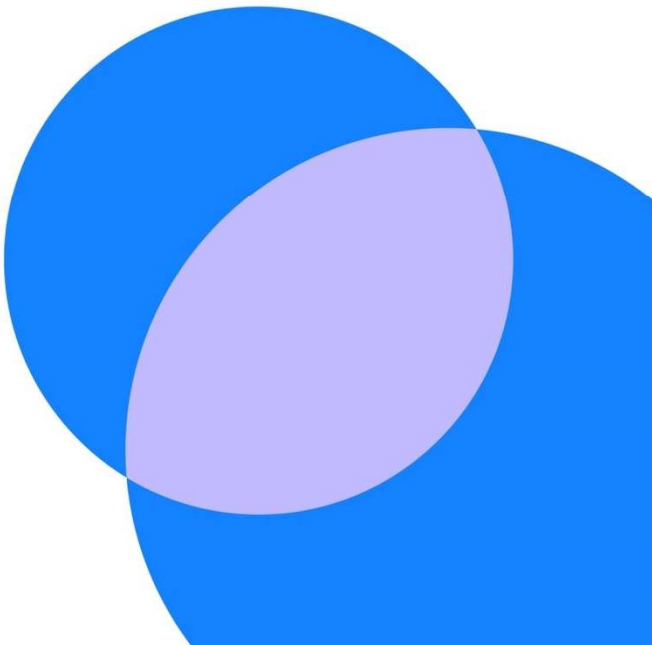
OFCOM CONSULTATION ON TELECOMS SECURITY AND RESILIENCE

CITYFIBRE RESPONSE



Introduction

1. We have been closely monitoring the progress of the Telecoms Security Act, and have already responded to the DCMS consultation on the draft Regulations and Code of Practice. We welcome the additional clarity provided by the DCMS consultation and associated materials, although as discussed below, we consider that there are still several outstanding questions of major importance which require further consideration by the Government.

2. Pending the outcome of that further consideration, we are not in a position to give definitive views on some aspects of this consultation. However, we broadly welcome the approach outlined by Ofcom, in particular the clear intent to approach monitoring and enforcement in a graduated way that recognises that providers will be on a 'journey to compliance'.

3. CityFibre has a strong internal culture of safeguarding network security and resilience and has already taken important steps to implement rigorous security procedures. But we recognise that the new TSA regime may require some further incremental measures to be implemented and of course Ofcom's proposals will involve a step-change in external reporting.

4. As we prepare for the Act's commencement, we will need greater detail on Ofcom's expectations in terms of certification/audit of compliance. Whilst Ofcom's consultation provides some helpful clarity, we would welcome early engagement with Ofcom to ensure that our roadmap on this aligns with Ofcom expectations.

Outstanding Policy Questions

5. In our response to its consultation we have asked the Government to consider the following matters:

Implementation timescales and tiering

6. The Government outlines a graduated approach to compliance based on a tiering system, which is also reflected in Ofcom's consultation. On the basis of the information available, CityFibre would expect to be placed in Tier 2. However CityFibre is in the (possibly unique) position of being a Tier 2 provider wholesaling to Tier 1 CPs (Vodafone and TalkTalk Group). The Government's consultation appears on the face of it to require Tier 1 providers to cascade their own security obligations through their supply chain, and to have completed this process by March 2023. This would mean that CityFibre's compliance journey had to align with Tier 1 timescales. Indeed, assuming our Tier 1 customers take some time to themselves determine their path to compliance and then seek to cascade to their customers, we may find ourselves with an even more foreshortened timeline to effect the necessary changes. Clearly, this undermines the Government's intent of creating a graduated compliance path for smaller operators. We have asked the Government to consider changes to its proposals to remedy this problem.

Mergers and acquisitions

7. M&A activity is widely anticipated to take place, particularly amongst the alternative fibre network (altnet) community, over the next two years. The Government's consultation appears to expect the acquiring operator to ensure 'day 1' compliance of any acquired assets, even if these were located in Tier 3 prior to the acquisition and hence at an earlier stage of their compliance journey. This may deter M&A activity which would otherwise lead to economically efficient industry consolidation and stronger infrastructure competition, whilst having the perverse effect of leaving customers on a smaller, inherently less secure network. We have urged the Government to make clear that an acquisition of this kind would then trigger a new 'compliance journey' relating to the acquired assets.

Stability

8. Whilst recognising that the threat landscape is constantly evolving, operators will need a reasonably stable baseline in order to plan and implement their compliance journey. We are therefore urging the Government to avoid further wholesale changes to the CoP and Regulations and to communicate as early as possible any possible evolutions in order to integrate these into operators' plans as seamlessly as possible.

Comments on Ofcom's draft general statement of policy under section 105Y of the Communications Act 2003

Compliance Monitoring

9. We support Ofcom's general approach of undertaking initial data-gathering using its s135 powers, complemented by direct engagement with operators.

10. As regards the tiered approach to monitoring, we welcome the slightly elongated timescales for Tier 2 operators compared with Tier 1, particularly time to respond to requests. Having said this, as already noted the Government's approach to supply chain assurance means that CityFibre may find itself effectively exposed to Tier 1 timescales for compliance. For this reason we would welcome the earliest possible engagement with Ofcom to discuss overall expectations and also what specific quantitative data sets Ofcom expects operators to furnish in s135 requests, so that we can start any systems development work and routine data capture.

11. As regards the more intrusive monitoring tools established by sections 105N-Q, we agree with Ofcom's intention to keep these firmly in reserve during the initial ramp-up phase of the new TSA regime.

Testing

12. CityFibre is already certified under ISO 27001 and the 'CyberEssentials' programme. We also conduct periodic penetration testing using external security specialist organisations. We have not, however, participated in TBEST. We would like an early opportunity discuss with Ofcom whether evidence of these existing processes would be sufficient to demonstrate compliance.

Reporting and Information sharing

13. CityFibre is generally comfortable with Ofcom's proposed approach. More broadly we think it is important to create a culture in which operators and public bodies share information about security threats and compromises, including emerging trends, in a 'safe harbour' context where such information is freely exchanged amongst relevant experts without reputational risk. There are existing frameworks established for such information-sharing between agencies (eg: ENISA CERT) and internet infrastructure operators. Ofcom should consider the establishment of a similar structural solution for information-sharing between infrastructure operators.

Comments concerning Ofcom's draft guidance on resilience requirements in sections 105A to D of the Communications Act 2003

14. CityFibre is building an entirely new full fibre network with resilience designed in from the outset, using fibre ring architecture and other functional characteristics that minimise single points of failure. We have comprehensive, state of the art real-time network performance monitoring processes in place that allow us to identify and rapidly rectify any resilience issues. We have also actively sought to ensure that our supply chain presents no resilience risks.

15. As a wholesale-only operator, our network resilience is reflected in industry-leading SLAs on network availability and reliability.

16. We will review whether existing processes for governance and accountability in respect of resilience need to be updated or further formalised.

17. We will also review all documentation referred to in Ofcom's guidance (eg: ENISA Technical Guidance on Security Measures) though our initial view is these reflect existing company practice.

18. As Ofcom is aware, CityFibre is making extensive use of Openreach civil infrastructure using the PIA product and also relies on other Openreach products such as Cablelink as ISP traffic handover points. We would welcome further dialogue with Ofcom to discuss how resilience risks associated with these products (for instance through the progressive upgrade of Openreach's pole estate) can be effected over time.

CityFibre
May 2022