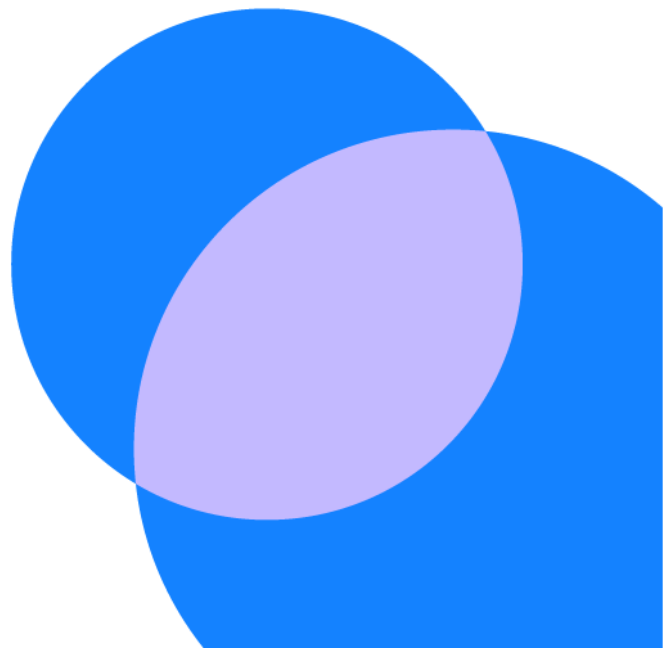


Consultation on Ofcom's draft general statement of policy under s105Y of the Communications Act 2003: CityFibre Response

August 2026



Summary

1. CityFibre agrees that Ofcom's approach to monitoring compliance with TSA obligations should evolve over time. The programme should now move beyond the regular requirements to provide s135 information responses in favour of more structured engagement between operators' technical security experts and Ofcom staff.
2. However, we are concerned that the adoption of an approach to compliance monitoring based on Assessment Notices risks imposing excessive burdens on operators. At minimum, Ofcom should put in place procedural safeguards around the use of Assessment Notices to minimise the burden they would impose on operators and to avoid compliance with Assessment Notices hindering the ongoing task of implementing TSA-compliant security measures.
3. We consider that the current drafting of the guidance places undue weight on participation in the voluntary TBEST programme. It appears to suggest that operators may be served with Assessment Notices if they choose not to participate in that particular programme.
4. We are concerned that the proposed changes to Security Compromise reporting guidance may lead to substantial over-reporting of relatively minor network outages. This should be addressed by redrafting the guidance to align more closely with the legal obligation placed upon operators to report 'significant' security compromises only. Ofcom should revisit its approach to the 'press coverage' qualitative reporting trigger, to avoid leading to reporting of incidents that are not significant.

Compliance Monitoring

Question 1: Do you have any comments on our proposed updates to our guidance on compliance monitoring?

5. Ofcom considers that the process of monitoring compliance with the TSA should now evolve, reflecting the relative maturity of the TSA and Ofcom's experience in monitoring the regime thus far. However, from an operator's perspective, the process of implementing TSA obligations is ongoing. Whilst CityFibre is on track to be fully compliant with TSA obligations, we are continuing to work through a range of issues arising, including the modification of all existing supplier contracts (an obligation which does not take full effect until 2027)¹. In addition, the Government's recent revisions of

¹ As set out in the explanatory text accompanying TSA Code of Practice measure M.10

the TSA Code of Practice impose additional obligations² which will now have to be assessed and (where necessary) integrated into our compliance activities on the timescales set out in that revised Code of Practice. The focus of our technical experts remains on ensuring the execution of programmes of activity designed to meet these evolving obligations.

6. Having said this, we agree with Ofcom that it is appropriate for it to move beyond s135 information gathering. As Ofcom recognises in the draft guidance, there is already scope for Ofcom to require follow-up meetings to discuss s135 responses,³ but CityFibre has, thus far, had very limited engagement with Ofcom in relation to TSA implementation. We would welcome deeper engagement with Ofcom technical experts to discuss implementation issues and challenges.
7. Ofcom should bolster the compliance monitoring programme with a regular structured dialogue with Tier 1 and 2 operators, to provide greater transparency of the focal areas of Ofcom's compliance programme and to set out in advance any specific matters of concern (eg: common themes emerging from analysis of s135 responses, or information about novel security threats). This could be done via a regular series of bilateral meetings with individual operators and/or through a contact group involving nominated security professionals from Tier 1 and Tier 2 companies. We consider that this would be an obvious next step on the TSA compliance implementation journey, recognising that Ofcom's and operators' aims are aligned on telecoms security, and moving to a collaborative dialogue on how to respond to emerging threats.
8. Conversely, we have significant concerns about the proposals set out in the consultation, specifically in relation to what appears to be an intention to make routine use of Assessment Notices. The scope of Assessment Notices as specified in s105O of the Communications Act 2003 allows Ofcom to impose obligations akin to an independent full security audit.
9. Ofcom notes that: *'Where we previously thought they [Assessment Notices] would likely represent an escalation in our concerns around compliance, we now think that in certain circumstances they could be a more appropriate and proportionate way to inform our assessment of how communications providers*

² In particular, updated and newly introduced technical specifications, including specific measures around test networks and services, privileged access workstations (PAWs), API management and signalling security controls, to be implemented between March 2028 and 31 March 2029.

³ Draft guidance document, paragraph 3.23

*are complying with their security duties*⁴ However, no evidence is presented to support this, nor are alternative iterative steps (such as the structured dialogue with operators we outline above) considered.

10. We believe Ofcom's previous interpretation of these powers as an escalation route to investigate an existing concern about compliance remains appropriate and proportionate.
11. We would be particularly concerned if Ofcom were to seek to impose obligations to conduct testing or allow a third party to undertake testing as part of an Assessment Notice. CityFibre is already undertaking an extensive process of security testing, both of systems and processes as required to maintain our security accreditations under Cyber Essentials and ISO 27001, and third-party penetration testing conducted by accredited third party organisations. It would be potentially highly disruptive to have to undertake alternative testing in order to comply with an Assessment Notice, alongside the extensive programme of activity already being undertaken. We also note that would be expected to bear the expense of such additional testing by virtue of section 105N(2)(b) of the Communications Act.
12. Overall it is clear to us that the business impact of complying with an Assessment Notice would be substantial, even were third party testing obligations not involved, as it would require key personnel to be diverted from day to day security operations. Hence, we disagree with Ofcom's assertion⁵ that adopting ANs will reduce the compliance burden on business, particularly as it is proposed to continue use of s135 Notices in parallel.
13. It is possible that Ofcom intends to use these powers in a relatively light-touch way. However, this is not reflected in either the consultation document or the associated draft guidance at present. If Ofcom maintains its position that it wishes to use Assessment Notices as part of its routine monitoring programme, then its guidance must provide greater clarity and procedural safeguards to ensure that the burden on operators is proportionate to Ofcom's aims. This should involve, at a minimum:
 - At least three month's advance warning of an Assessment Notice being issued, and the opportunity for operators to comment on the scope of the request⁶. We note that Ofcom has the power to issue an Assessment

⁴ Consultation document, para 3.13

⁵ Consultation document, para 3.14

⁶ We note that, at paragraph 3.39 of the draft guidance, Ofcom states that it may share drafts in advance where 'it is appropriate to do so.' We consider that as a matter of regulatory best practice Ofcom should always share draft ANs in advance, in the same way that it does s135 notices.

Notice with an Urgency Statement under section 105P where the need to undertake an assessment is time critical. For Assessment Notices issued under s105N there is no reason why appropriate advanced notice and an opportunity to comment on a draft should not be offered.

- Information Notices that impose obligations in relation to third-party testing should be kept to a minimum. As discussed further in the next section, Ofcom should be mindful of the extensive existing testing programmes being conducted by operators. Further testing as an element of an Assessment Notice should be considered only where an operator has been unable to demonstrate, via its s135 filings, that it is already compliant with TSA Regulation 14.

Testing

Question 2: Do you have any comments on our proposed updates to our guidance on testing?

14. A key principle of the TSA is that operators have flexibility in how they demonstrate compliance with specific measures. This is reflected in the language of both TSA Regulation 14, and the associated guidance in section 13 of the Code of Practice, which states that '***an** example of this type of testing is Ofcom's TBEST scheme*'.

15. The proposed wording of the guidance states that:

*'Ofcom operates a voluntary, collaborative testing programme called TBEST. Regular voluntary TBEST participation may reduce the likelihood that testing will be required under section 105O for the purposes of an assessment under section 105N, as it provides assurance on the effectiveness of a provider's overall security controls.'*⁷

16. This can be construed as giving TBEST a quasi-obligatory status, as it implies that non-participating companies may in effect be forced to participate either to avoid an Assessment Notice, or (potentially) will have an Assessment Notice imposed which requires them to participate in TBEST. This is clearly inappropriate given that TBEST remains a voluntary programme, and having regard to the flexible character of the TSA legal obligations on testing as outlined above.

⁷ Draft guidance document, paragraph 4.7

17. The context for our comment is as follows. CityFibre recognises the importance of third-party penetration testing as a key means to identify potential vulnerabilities and take appropriate remedial measures. We already undertake periodic testing of this kind using CREST-accredited bodies.⁸ Given this, CityFibre considers that we are fully compliant with the relevant obligations placed upon us by the Regulation 14 of the TSA.
18. CityFibre has chosen not to participate in TBEST hitherto. There are at present only a limited number of third-party testing organisations accredited to undertake TBEST, with what we understand to be long lead times of twelve months or more to undertake testing. In addition, based on our understanding of the focus of TBEST, we have concluded that at present the CREST-accredited bodies we utilise provide a more appropriately tailored examination of our business's potential vulnerabilities. We are not aware of specific threats or risks which TBEST would seek to test for that are not covered by the testing activities already being undertaken.
19. Whilst we do not rule out participating in TBEST in the future, this is not at present part of our TSA compliance roadmap, and it would be costly, burdensome and disruptive to our existing third-party testing programme to now have to superimpose TBEST participation on top of this.
20. Ofcom should revise the text of the guidance to remove any suggestion that participating in TBEST is required to avoid the imposition of an Assessment Notice.

Incident Reporting

Question 3: Do you have any comments about our proposed changes to our security incident reporting thresholds and criteria, as described in paragraphs 3.19 to 3.48?

21. The proposed changes to the guidance risk creating material uncertainty as to what types of 'security compromise', and on what timescale, Ofcom now expects to be reported to it. We are cognisant of the legal obligations placed upon us as an operator to report Security Compromises which are significant in scale under section 105(K) of the Communications Act 2004 and would take appropriate action in the event of any such incident occurring. In doing so, we would have regard to Ofcom's quantitative and qualitative thresholds as set

⁸ <https://www.crest-approved.org>

out in the guidance, but it is important that the guidance closely reflects the underlying legal obligation on us and does not extend beyond this.

22. On qualitative reporting thresholds, CityFibre considers that the guidance needs to take a different approach to press reporting in its list of qualitative factors triggering a reporting requirement. CityFibre has raised concerns about this issue under the existing guidance, but our concerns are amplified by Ofcom's proposal that any press reporting of an incident should trigger a 'critical' report within three hours of the incident occurring.⁹
23. Press coverage is not a factor mentioned in section 105K of the Communications Act 2004 from which our obligation to report 'significant' security compromises derives. Ofcom's inclusion of press coverage on its list of reporting triggers predates the current legislation, and, to the extent that we understand the logic of its retention in the new guidance, must rest on an assumption that press coverage is a proxy for 'significance'. However, this logic is poor when it comes to local and trade press. Local press may judge a relatively minor resilience incident (eg: a network strike or damage to a pole affecting a handful of customers) to be newsworthy if, for example, it leads to a temporary road closure. Similarly, some trade press sources may pick up on relatively trivial network outages and report them simply because they bulk out their news agenda on an otherwise quiet day. A clear example of this has arisen under the existing guidance where Ofcom has asserted that a report of a CityFibre network outage in the online trade news outlet 'ISP Review' should have been reported to Ofcom, notwithstanding that the incident in question did not meet any other quantitative or qualitative reporting thresholds.
24. Furthermore, as Ofcom does not define 'local and trade media', this inevitably causes material uncertainty on what it judges to qualify in these categories. For example, does 'trade media' include the proliferation of specialist news sites, blogs and user forums established in recent years with a telecoms industry focus, such as (but not limited to) ISP Review? Does local media include citizen journalism or posts on community Facebook pages?
25. In our view the 'media coverage' category should be removed altogether from the list of qualitative triggers for reporting, because it has no legislative underpinning in section 105K of the Act. Alternatively, the list of 'critical

⁹ The list included in paragraph 5.28 of the draft guidance includes both 'Security compromises attracting local, national or trade media coverage, regardless of whether they meet the quantitative thresholds in Tables 1, 2 and 3' [bullet 2] and 'Security compromises attracting national mainstream media coverage, regardless of whether they meet the quantitative thresholds in Tables 1, 2 and 3' [bullet 5]. It is unclear why national media appears in both bullets.

incident reporting' factors at paragraph 5.28 of the guidance should be limited to national media only.

26. In relation to the bulk reporting requirements for 'moderate' reportable incidents (ie: those that do not trigger the 72-hour or 3-hour reporting requirements), it is not clear to CityFibre what incidents Ofcom is expecting to be rolled up into such bulk reports. On one reading of the guidance, the expectation is that any resilience incident which leads to any loss of services to customers *at all* should be included in bulk reports. This would impose a very substantial burden on operators to submit what could easily run into hundreds of reports of minor network outages, such as damage to poles or fibre network strikes, which affect only a handful of customers.
27. We assume that it is not Ofcom's intention to receive large volumes of such reports and we would therefore encourage Ofcom to clarify what constitutes a 'moderate' security compromise, establishing a de minimis quantitative threshold, such that only reporting of security compromises which have significant impact on service availability need to be reported.

Reporting Templates

Question 4: Do you have any comments about the proposed changes to our reporting templates?

28. We have no comments on the revised Major Incident reporting template.
29. We do have significant concerns, however about the proposed bulk reporting template. This reflects our general uncertainty, referred to in the previous section, of what types of incident Ofcom is expecting to be reported using this format. In our view, the scope of the information required to be provided using this template, which is only slightly less extensive than that required in the Major Incident template, would be disproportionate if it has to be completed for all types of resilience incident, no matter how minor in scope.