

## Consultation: Proposals to update our General Statement of Policy under section 105Y of the Communications Act 2003

4 August 2026

### Introduction and overall position

techUK is the UK's leading technology membership organisation, with around 1,100 members. Our Telecoms Programme convenes network operators, equipment vendors and other communications providers on the policy and regulatory framework for UK digital infrastructure. This response reflects the consolidated views of that membership. Not every member holds the same view on every point, and where views diverge materially, we have said so.

We support the objectives behind this review. Strengthening the resilience and security of UK networks, and improving the quality and consistency of incident reporting, are the right aims, and it is sensible for Ofcom to revisit guidance that has been in force for more than three years in the light of operational experience. Our comments are offered constructively and are directed mainly at the detail of the proposals rather than their direction.

Three themes run through our answers. First, some of the proposals carry costs that Ofcom's impact assessment understates, most notably the new rural cell-site threshold and the monthly Radio Access Network (RAN) data requirement, and we ask that these are held consistently to the Growth Duty and draft Statement of Strategic Priorities that Ofcom cites in Annex 2. Second, several of the reporting proposals attach urgent or costly obligations to factors that the reporting provider cannot readily observe or control, including media coverage, the physical repair time of remote rural sites, and cell-site data held only by a host MNO; this is a particular problem for MVNOs and wholesale-dependent providers. Third, where changes require new systems, a defined lead-in period from the autumn 2026 statement is needed before they take effect.

### Question 1: Compliance monitoring

#### ***Do you have any comments on our proposed updates to our guidance on compliance monitoring?***

techUK supports the move towards a more proportionate, risk-led supervisory model, and in particular welcomes the proposed change in the typical cadence of section 135 information notices from around nine months to twelve. In our members' experience the nine-month interval has proved unrealistic once time is allowed for comment on draft notices, for those comments to be reflected, and for providers to prepare substantive responses. Twelve

months is a more honest reflection of how the cycle has worked in practice, and it will ease the resourcing pressure on provider compliance teams.

We have more significant reservations about the proposal to make greater, more routine use of assessment notices under sections 105N to 105Q. Assessment notices are a highly intrusive instrument. The powers under section 105O extend to requiring providers to carry out or arrange system tests, to make staff available for interview, and to permit authorised persons to enter premises to inspect equipment, documents and information. In our members' view this instrument is better suited to cases where Ofcom has a *prima facie*, case-specific basis for concern that a provider may not be complying with its duties, rather than serving as a routine or default means of gathering information alongside, or in place of, section 135 notices.

We would also question the suggestion at paragraph 3.14 of the consultation that assessment notices may be less burdensome than information notices. In many cases the opposite will hold. System tests, staff interviews and premises visits are frequently more resource-intensive and more operationally disruptive than preparing a written return, and they need considerably more time to arrange. Burden is highly case-specific and should not be presumed lower.

A related concern is the way these instruments are being used in combination. The indication from Ofcom is that it intends to pair interviews with information requests on the same topic: a meeting is requested on the basis of a set of questions, and is then followed by an RFI covering that same ground so that Ofcom can hold a formal record. From a provider's perspective this is double-handling of a single topic, and it roughly doubles the impact. The overhead of responding has risen substantially and now requires dedicated resource over and above the operational teams who hold the underlying knowledge. If Ofcom does adopt a more supervisory model, we ask that it avoids duplicating the same enquiry across an interview and a subsequent RFI, and instead uses a single route to a formal record wherever possible.

If Ofcom does intend to make broader use of these powers, we ask for transparency and predictability about how it will choose between them. We would welcome published criteria describing when Ofcom will use an assessment notice rather than an information notice or a section 105I direction; an indication of the steps Ofcom will take before issuing an assessment notice, including whether a provider will normally have the opportunity to address Ofcom's concerns through correspondence or a section 135 notice first; and an explicit, auditable commitment that assessment notices will not be used as a default position or as a fishing exercise. We welcome the commitment at paragraph 3.39 to share draft assessment notices for comment, and ask that this becomes standard practice rather than something done only where appropriate, with adequate time built in for providers to prepare.

## Question 2: Testing

***Do you have any comments on our proposed updates to our guidance on testing?***

techUK supports the proposal to shorten the testing section of the Statement of Policy and to direct providers to the Code and to the TBEST handbook for the detail. Maintaining the same material in several places has previously created a risk of the documents falling out of step with one another, and consolidating the detail should reduce the need for future amendment. We ask only that the cross-references are kept clear, current and version-stable, so that changes to the Code or the TBEST handbook do not open gaps or ambiguities in the Statement of Policy, and that a short signpost at the start of the section explains what each referenced document covers. That would help smaller providers, who tend to use the Statement of Policy as their main reference point.

Our substantive concern relates to the interaction between the testing section and the proposed wider use of assessment notices discussed under Question 1. Paragraph 4.7 states that regular voluntary TBEST participation may reduce the likelihood that testing will be required under section 1050. Read on its own, this is unobjectionable. Read together with Ofcom's intention to make greater use of assessment notices, however, it carries an unwelcome implication: that providers who choose not to take part in TBEST may face a materially greater likelihood of mandated testing under an assessment notice, so that Ofcom can obtain equivalent assurance by another route. That risks making TBEST a de facto requirement, notwithstanding its formally voluntary status.

TBEST may be a suitable and proportionate assurance mechanism for some operators, but it is not necessarily the most appropriate approach for every organisation, given differences in network architecture, risk profile, scale and the assurance arrangements a provider may already have in place. We therefore ask Ofcom to confirm in the final Statement of Policy that participation in TBEST is genuinely voluntary; that non-participation will not, of itself, be treated as a factor increasing the likelihood of an assessment notice; and that Ofcom will give equivalent weight to alternative, comparable third-party assurance arrangements when considering whether further testing is needed.

### Question 3: Security incident reporting thresholds and criteria

***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?***

This is the area of greatest concern to our members. We support the drive for consistency and a clearer taxonomy, but we have substantive concerns about the rural cell-site threshold, about the observability of the new metrics for MVNOs, about the volume implications of the new thresholds, and about the use of media coverage as a trigger for critical classification. We take each in turn below.

#### Consistency and taxonomy

We agree that the previous approach of agreeing bespoke Major Service Failure definitions with each MNO individually has produced inconsistent reporting between operators, and we

support replacing it with a single set of universal criteria. We also welcome the relabelling of the severity categories from urgent, non-urgent and non-major to critical, major and moderate, which aligns better with the language operators already use internally. We ask Ofcom to confirm, as it states, that this is a change of terminology only, and that it carries no unintended operational reclassification of incidents and no change to reporting timeframes.

## The rural single cell-site threshold (our primary concern)

Our members' main concern is the proposed threshold of one or more rural cell sites lost for eight hours or more. We recognise the legitimate, consumer-focused rationale. Rural areas have lower mast density and less overlap between sites, mast-sharing under the Shared Rural Network (SRN) is common, and the loss of a single rural site can isolate a community, including its ability to reach the emergency services. Our concerns are with the cost, the methodology and the proportionality of the proposal as drafted, rather than with the underlying aim.

First, we consider the cost to be materially understated. Ofcom's own impact assessment, at paragraph A2.17, accepts that operators do not currently differentiate between urban and rural cell sites. Identifying rural sites for reporting purposes is therefore a genuine new capability build, carrying both capital and operating cost, rather than the low or immaterial cost implied elsewhere in the impact assessment. We ask Ofcom to revisit this finding in the light of the member evidence we will provide.

Second, the proposed method of determining rurality is a weak proxy for the effect on customers. Classifying a site by the postcode of the mast's physical location does not reflect the area the site actually serves. Masts are frequently placed on high ground or beside trunk routes whose postcode classification differs from that of the population served, so a site-postcode measure risks both overreporting and underreporting. A measure based on the area served, rather than the location of the mast, would more accurately capture the impact the threshold is intended to address.

Third, the eight-hour trigger interacts poorly with the practical realities of rural site maintenance. Rural and most-rural sites are inherently slower and harder to restore than urban ones, for reasons of engineer travel time, difficult access in poor weather, single and often non-resilient power feeds, and microwave backhaul with limited redundancy. Adverse weather also carries a genuine safety dimension: reaching a remote site in a storm or flood can place engineers at real personal risk, and a reporting threshold should not create pressure to attempt restoration in conditions where the responsible course is to wait for access to become safe. Outages that would be resolved comfortably within eight hours at an urban site will routinely exceed eight hours in remote areas for reasons of geography and access, and not because of any resilience or security failing on the operator's part. As drafted, the trigger will therefore capture a disproportionate share of ordinary rural maintenance events, inflating report volumes without a corresponding signal of significance. We ask Ofcom to consider

whether a longer duration, or one calibrated to realistic rural restoration times, would better target genuine rural isolation.

Fourth, the dataset itself requires governance. It combines three national classification systems of differing methodology and vintage, being England and Wales from 2021, Scotland from 2022 and Northern Ireland from 2015, and it involves judgement in mapping them onto a single three-point scale, for example in condensing the Scottish six-point scale. We ask Ofcom to publish the full mapping and its treatment of boundary cases, to set out how often the dataset will be updated and how providers will be notified of changes, and to provide a mechanism by which providers can verify and challenge the classification of individual sites.

Fifth, the threshold raises questions of volume against significance, compounded by the SRN. A trigger set at a single rural site for eight hours could generate a high volume of individually low-significance reports. Because SRN sites share common power and, in some cases, common backhaul, a single physical failure at one shared mast can simultaneously breach the rural threshold for every MNO present on that site, producing three or four separate reports of the same event; Ofcom acknowledges that duplicate reporting may result. We ask Ofcom to confirm how it will de-duplicate such reports, for example whether a single report from the site's lead or host operator, identifying the affected MNOs, would discharge each operator's obligation for that shared-site event.

Sixth, the Resilience Guidance now supports this position. Ofcom published its Network and Service Resilience Guidance for Communications Providers on 16 June 2026, superseding the 2022 guidance. That document acknowledges that the access and last-mile domain is likely to contain single points of failure and that highly resilient access networks are costly to build (sections 3.3.1 and 4.2.1), and that some legacy 2G and 3G RAN components may not support the automatic failover mechanisms expected of 4G and 5G networks (section 4.2.1, footnote 32). These acknowledgements reinforce our submission that extended single-site rural outages frequently reflect geography, access and legacy-technology constraints rather than any resilience or security failing on the operator's part.

## The cell-site (urban and semi-urban) thresholds

We regard the proposed thresholds of twenty-five or more sites for two hours, and one hundred and fifty or more sites for any duration, as a reasonable and objective measure of scale in principle. Two points of detail matter a great deal to how they will operate. The first is the counting basis. If sites are counted per logical cell, per sector, or per technology (2G, 3G, 4G and 5G) rather than per physical site, a failure at a small number of physical locations could be counted as twenty-five or more sites, capturing events much smaller than the threshold appears to target. We ask Ofcom to define the counting basis unambiguously, and to define how the same area is delineated for the twenty-five-site trigger. The second is that a two-hour window is short relative to common transmission faults. Backhaul-ring and transmission failures affecting many sites at once are frequently restored within two to four hours, so a twenty-five-site, two-hour trigger may capture routine, quickly-resolved events. We

ask Ofcom to consider whether a slightly longer window would better target significant outages while excluding transient faults that are already being managed within normal operational timescales.

## MVNOs and wholesale providers cannot observe the new metrics

The new cell-site and rural thresholds are expressed in units that only the host MNO holds, namely which sites have failed, how many, their rural classification, and their global cell IDs. An MVNO has no independent visibility of its host's radio network and typically receives no real-time, site-level failure feed from it. Yet paragraphs 3.45 and 5.21 require the MVNO to collect the relevant information and report it itself, and prevent it relying on the host to report on its behalf. As drafted, this obliges MVNOs, and other wholesale-dependent providers, to report against metrics they cannot observe, and it will produce systematic duplicate reporting, as the host and each affected MVNO report the same underlying event.

We ask Ofcom to clarify what standard of site-level information an MVNO is realistically expected to obtain from its host, and within what timescale; to confirm whether a host-provided incident reference or data feed can discharge the MVNO's cell-site and rural reporting obligations, leaving the MVNO to report only its own customer-impact view; and to set out how it will handle the resulting duplicate reports. We would also welcome Ofcom's view on whether a minimum incident-data-sharing expectation between hosts and MVNOs should be reflected in wholesale access arrangements, so that the duty placed on MVNOs is capable of being met in practice.

## The catch-all for significant incidents

We understand that the clarification at paragraph 3.41, that incidents with a significant effect remain reportable even where they meet no specific threshold, is intended to reflect the underlying duty in section 105K rather than to create a new obligation. Presented as a standalone catch-all in the guidance, however, and without further explanation of what a significant effect outside the specified thresholds might look like, it creates real uncertainty for providers applying the guidance, and it is likely to encourage defensive over-reporting. We ask Ofcom to provide qualitative guidance or worked examples of the kinds of incident it has in mind, so that the standard can be applied consistently.

## Wholesale and resale scope

More generally, where a provider relies on a third party's network to deliver its service, we consider that any duty to collect and report information about that network should be qualified by a reasonable or best endeavours standard, reflecting the practical limits on what such a provider is able to obtain from its upstream network provider.

We also ask Ofcom to clarify the scope of the reporting obligations as they apply to wholesale supply. Although paragraph 5.21 confirms that a provider is not expected to alter its monitoring or reporting systems merely to ascertain end-customer numbers, and that the obligation is triggered only where it is clear to the provider that a threshold will be exceeded, the consultation does not address whether a wholesale-only service supplied exclusively to other communications providers constitutes a “public” electronic communications service for these purposes. We would welcome confirmation on this point, together with clarification of how resale arrangements, for example mobile service resale, should be treated within the reporting framework.

## The volume and burden of monthly bulk reporting

More generally, members are concerned about the cumulative administrative burden of including all moderate incidents in monthly bulk reports once the new cell-site and rural thresholds take effect. Where an incident falls well below the customer-impact levels that have historically warranted regulatory attention, and is captured only because of the new infrastructure-based criteria, it is not clear that the benefit to Ofcom of receiving and processing a much higher volume of such reports is proportionate to the effort involved in identifying, recording and submitting them. We ask Ofcom to monitor the volume of bulk reports generated under the revised thresholds, and to consider a de minimis exemption, or a simplified aggregated format, for very low-impact moderate incidents.

## The critical threshold

The stated purpose of reducing the critical threshold from three million to 1.5 million user-hours is to capture incidents across the range of Tier 2 MVNO subscriber bases. Like the percentage-based threshold we flag above, this risks bringing smaller providers into the critical band on the basis of their relative size rather than the absolute customer impact of an incident, which may be low. Halving the threshold will also roughly double the population of incidents falling into the critical band, each of which carries a three-hour initial notification that will often fall outside office hours. NOC and security-incident teams are a largely fixed resource, and a material increase in out-of-hours critical notifications draws that resource towards regulatory notification at precisely the point it is most needed to manage the incident itself. We ask Ofcom to justify the recalibration against absolute customer harm rather than subscriber-base coverage, to model the expected change in critical-notification volume, to monitor it after implementation, and to confirm that the change will be reviewed if it inflates urgent reporting disproportionately to any increase in customer harm.

## Media coverage as a trigger for critical classification

We have significant concerns about the proposal at paragraph 5.28 to classify any incident attracting local or trade media coverage as critical, triggering the three-hour notification requirement regardless of whether it meets any quantitative threshold. Media coverage is not

a reliable proxy for the severity or customer impact of an incident: it does not automatically make an incident critical regardless of operational thresholds and therefore cannot of itself lead to a security compromise being reportable under section 105K(1). Members tell us that, therefore, it is outside Ofcom's powers for the guidance to make such incidents reportable automatically. Furthermore, minor, quickly-resolved incidents can attract disproportionate attention for reasons unrelated to their technical significance, while some genuinely serious incidents attract little coverage. Attaching a statutory reporting consequence to a factor entirely outside the provider's control, and unrelated to the actual impact of the incident, risks obliging operators to make urgent notifications before they have had a reasonable opportunity to establish the facts, and so to submit inaccurate or speculative initial reports.

The trigger also imposes an unworkable monitoring burden. Monitoring national press is feasible, but tracking the full range of local and trade outlets is not, and the overhead of attempting to do so is disproportionate. Much of this coverage is published at a frequency and level of detail that offers no real signal, and the incidents it reports would frequently never approach a reporting threshold on customer-hours. A provider cannot reliably know, in the three-hour window, whether an incident has been picked up somewhere in local or trade media, which makes the obligation impossible to discharge with any confidence.

We ask Ofcom to remove local and trade media coverage as an independent trigger for critical classification. We also ask Ofcom to confirm that providers can give notification of an incident by email, as an alternative to calling a dedicated 24x7 telephone number. During a genuinely critical incident operational and senior staff will be focussed on fixing the issue and restoring services and an email may be less demanding at that point than having to call and potentially answer Ofcom's questions.

## Other clarifications

We welcome the further clarifications on pre-positioning security compromises, on 112 and 999 access while roaming, on third-party reporting responsibilities, and on the linking of geographically dispersed severe-weather outages. Each addresses a genuine point of ambiguity raised by industry in the past. On severe weather in particular, aggregating dispersed sub-threshold outages into a single reportable incident is operationally complex, and we would welcome practical guidance on how providers should aggregate such events, and over what time window.

## Question 4: Reporting templates

### ***Do you have any comments about the proposed changes to our reporting templates?***

techUK welcomes some of the proposed template changes, which reflect feedback from industry. Embedding explanatory text in the template should make reporting clearer, particularly for providers who report infrequently, and should reduce the need to maintain separate internal processes for each. We support the addition of the third-party details, global

cell IDs and other notes columns in principle, since each should improve Ofcom's understanding of an incident's impact.

We would raise three practical points. First, lengthening the form, while helpful for clarity, could slow completion of the initial notification when a provider is under the time pressure of an active critical incident. We suggest that Ofcom retain a short-form option for the initial three-hour critical notification, confirming awareness and giving a brief indication of the nature and scale of the incident, with the fuller, explanation-rich template reserved for the 72-hour report, consistent with the process already set out at paragraph 5.26. Second, for the global cell IDs field, we ask that the template allow bulk or summary submission, for example as an attached list or file reference, rather than requiring individual entry for incidents affecting a large number of sites, which would be onerous during a live incident. Third, we ask Ofcom to provide clear field-level guidance on what is expected in the new third-party details and global cell IDs columns, and to what level of detail.

The proposed bulk reporting template appears to require a level of detail closer to higher-priority incident reporting. For moderate or bulk incidents, this could require significant input from IT service, incident management and operational teams without a clear corresponding benefit. Members request that Ofcom explains why bulk reports need the same or similar level of detail as 72-hour reports, and should distinguish more clearly between information required for immediate regulatory action and information useful for later trend analysis.

Given how much the usability of the template affects the speed and completeness of the information that reaches Ofcom during an incident, we would encourage Ofcom to pilot the revised templates with a small group of provider volunteers before finalising them; to publish the final templates in locked form with field-level guidance, retaining the optional status of the third-party details, global cell IDs and other notes columns so that they do not become mandatory or de facto expected in practice; and to allow a reasonable transition period before they take effect.

## Question 5 (for MNOs): Monthly RAN cell list

***Do you have any comments about the requirement to provide us with a list of your RAN cells for purposes of mapping incidents and their impact?***

Our MNO members support the objective of enabling Ofcom to map incidents accurately using global cell IDs, and recognise that broadly equivalent RAN data is already compiled and shared with other recipients on a monthly basis. Our concerns are about the security sensitivity of the dataset, the extent of the data requested, and the way in which the requirement is characterised.

The central concern is security, and it sits in some tension with the purpose of the framework itself. The cell data reporting standard requests node IP addresses at fields 30 and 37, MME and AMF identifiers at fields 31 and 38, and a complete national inventory of sites with precise

locations and addresses. A monthly, comprehensive, national RAN dataset of this kind is exactly the sort of asset the security framework exists to protect. Consolidating every operator's dataset at a single regulator also creates a new and concentrated national target that does not at present exist in any single place. Members will want to be satisfied that the benefit to incident mapping clearly outweighs the risk created by assembling this data.

That points directly to data minimisation. For the stated purpose, which is to correlate a global cell ID in an incident report with a physical location, Ofcom needs the cell identifier and the location fields, not the full set of forty. The node IP addresses at fields 30 and 37, the core-network identifiers at fields 31 and 38, and similar operational parameters are not required to map an incident to a place, and they materially increase both the sensitivity of the dataset and the consequences of its loss. We ask Ofcom to justify each field it requires against the mapping purpose, and to omit those that are not essential to it.

We would also welcome detailed assurances on handling. The draft Statement of Policy refers at paragraph 3.24 to a secure platform for section 135 information, but it does not explicitly extend that commitment to the new monthly RAN submission. We ask Ofcom to confirm the secure transmission and storage arrangements for this dataset, to set out its retention period and its access-control approach on a least-privilege basis, and to explain the basis for any onward sharing with DSIT or the NCSC under the section 393 gateways.

The suggestion at paragraph 3.55 that MNOs could meet the requirement simply by adding Ofcom to an existing distribution list understates the position. The feeds members currently produce may differ in scope, format and frequency, and the security posture of their existing recipients may differ from Ofcom's. Adding a regulator as the recipient of a sensitive national dataset is neither cost-free nor risk-free. We ask Ofcom to confirm the legal basis on which the data is required, which we assume to be section 135, and to satisfy itself that the associated costs and risks have been properly assessed.

Finally, we ask Ofcom to confirm the versioning and stability of the cell data standard, and to commit to a defined process and notice period for any future changes to it, since operators will need to build and maintain automated monthly extraction processes that conform precisely to the specified field order and to the delimiting and escaping rules. Because this is a new recurring obligation rather than an incident-triggered report, we also ask for a settling-in period covering the first two or three monthly cycles, during which formatting or completeness issues arising from the transition to a new automated process would not attract compliance consequences.

## Cross-cutting points

Beyond the individual questions, we would highlight four cross-cutting points. On proportionality and the Growth Duty, we ask Ofcom to hold the rural-site and RAN-list proposals in particular to the Growth Duty and the draft Statement of Strategic Priorities it cites at Annex 2, given their bearing on investment in coverage and resilience, including the

rural objectives of the Shared Rural Network. On cumulative burden, we ask Ofcom to consider these changes alongside the Code of Practice, the Resilience Guidance and Connected Nations reporting, rather than in isolation. On implementation, we ask for a defined lead-in period from the autumn 2026 statement before the new thresholds and templates take effect, proportionate to the systems work involved in rural-site identification, the RAN feed and the template changes. And on the impact assessment, we would offer member evidence to test Ofcom's recurring conclusion that the changes carry no material cost, particularly for the rural threshold and the RAN dataset.

On the interaction with the Resilience Guidance, we note that the Network and Service Resilience Guidance for Communications Providers published on 16 June 2026 does more than sit alongside the framework under review: it operationalises the current section 105Y reporting thresholds as network design targets. Section 4.2.2 states that the user-hours-lost figure underpinning the reporting thresholds is a useful architecture, design and operational target to stay below, reproduces the current worked example of 80,000 user-hours (10,000 customers for eight hours), and cross-refers by footnote to the fixed and mobile numerical threshold tables in the Procedural Guidance. The consequence is that the threshold changes proposed in this consultation, in particular the reduction of the critical threshold to 1.5 million user-hours and the new infrastructure-based cell-site and rural triggers, are not confined to the reporting process. If adopted, they will leave the design targets that providers are expected to build against, as set out in the now-final Resilience Guidance, misaligned with the reporting obligations they are meant to mirror and potentially introduce through the Procedural Guidance completely new resilience obligations for thousands of RAN sites.

We therefore ask Ofcom to confirm whether providers will be assessed against the previous or the revised thresholds. Assessing providers against the revised infrastructure-based thresholds will affect the proportionality of these reporting proposals and should be expressly excluded.

Underlying several of the reporting proposals is a common issue that we ask Ofcom to address directly. Media coverage, the physical repair time of remote rural sites, and, for MVNOs, cell-site data held only by the host, are all factors outside the reporting provider's control or observation. We ask Ofcom to re-examine each proposal against the principle that a reporting obligation should turn on factors the reporting provider can actually observe, control or reasonably influence.