

Substantial Group Limited

167 – 169, 5th Floor,
Great Portland Street,
London,
England,
W1W 5PF

Ofcom Consultation: Proposals to update Ofcom’s General Statement of Policy under section 105Y of the Communications Act 2003

1. Executive Summary

1.1 Introduction

Substantial Group Limited welcomes the opportunity to respond to Ofcom’s consultation on its proposed update to the General Statement of Policy under section 105Y of the Communications Act 2003¹ (the “Consultation”). The telecoms security framework has now been in operation for several years and it is appropriate that Ofcom updates its supervisory and incident-reporting approach in light of that experience. We are supportive of the objective of clearer, more consistent and risk-based supervision.

Substantial Group companies build and operate full fibre networks and provide broadband services (consumer and business), digital voice, as well as business connectivity services. Those services are delivered over a shared Multi-Service Network (“MSN”) architecture. The section 105Y framework is relevant to providers of Public Electronic Communications Networks (“PECN”) and Public Electronic Communications Services (“PECS”), and the way in which Ofcom applies the framework therefore matters across our network and retail operating models. A single security compromise can affect more than one service, business connectivity is not naturally measured in residential end-user terms, and important information may sit with a supplier, wholesale customer or other third party during the early stages of a security incident.

1.2 Substantial Group’s position

Substantial Group is broadly supportive of Ofcom’s proposals. Our main requests are that the final Statement should:

- apply assessment notices in a targeted and proportionate way, taking account of cost, operational risk and existing assurance evidence;
- set out the fixed-network evidence supporting the proposed reduction in the critical severity threshold from 3 million to 1.5 million user-hours and remove the drafting ambiguities at the severity boundaries;

¹ [Consultation: Proposals to update our General Statement of Policy under section 105Y of the Communications Act 2003](#)

- clarify the treatment of repeat incidents, severe weather, below-threshold significance, pre-positioning, third-party information and qualitative reporting criteria so that providers can apply the rules consistently during a live incident;
- provide a clear and consistent method for counting affected customers and user-hours across broadband, digital voice, wholesale services and business connectivity, including leased lines;
- ensure the revised reporting templates accommodate estimates, unknown information and progressive updates, with clear timestamps, a stable bulk-reporting schema and a secure submission route for sensitive information;
- work with the Information Commissioner's Office ("ICO"), National Cyber Security Centre ("NCSC") and Department for Science, Innovation and Technology ("DSIT") to reduce duplicate incident reporting through common core fields and practical cross-referencing, while preserving each statutory reporting duty; and
- allow a practical transition for new reporting processes and templates.

2. Responses to Consultation Questions

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

Substantial Group supports Ofcom's proposal to reflect the maturity of the regime, including the move from an indicative nine-month to twelve-month cycle for regular section 135 information notices and the use of a broader supervisory toolkit. A more targeted approach should reduce burden where Ofcom focuses on the risks and controls that matter rather than repeatedly seeking broad descriptions of a provider's overall compliance position.

Assessment notices

We accept that assessment notices can be an appropriate supervisory tool and need not indicate an escalation in Ofcom's concerns. The safeguards around their use nevertheless matter. An assessment can require testing, interviews and access to premises, and providers are required to meet Ofcom's reasonably incurred assessment costs. For a live full fibre network those activities can also engage third-party facilities, outsourced functions and production systems.

Substantial Group's position is that Ofcom should:

- consider whether the regulatory objective can be achieved through less intrusive information gathering or voluntary engagement and, where an assessment notice is used, explain the principal risk or control area and why the notice is proportionate;
- scope testing, interviews, premises access and information requests narrowly and take account of operational and customer-impact risk;
- take both provider-side costs and Ofcom's or an assessor's costs into account when assessing proportionality, with reasonable visibility of likely scope and cost where practicable;
- reuse relevant assurance evidence, including independent audits, penetration tests, control testing and supplier assurance, where it addresses the same objective; and
- avoid seeking again evidence already provided through section 135 monitoring or other telecoms security supervisory activity.

Annex 7 already states that Ofcom will send draft assessment notices for comment where appropriate. We support that approach and would expect it to be the normal mechanism for

identifying avoidable scoping or operational issues before a notice is finalised, save where urgency makes that inappropriate.

Alignment with the Code of Practice

The final Statement should remain consistent with the Telecommunications Security Code of Practice 2026 (version 1.1). The Code recognises that appropriate and proportionate implementation depends on the provider's circumstances and that the Code is not the only means of compliance. Ofcom's supervision should preserve that outcome-based approach rather than turn individual Code measures into a mechanistic checklist.

Ofcom's 2024–25 Security Report² ("the Report") provides a useful practical example. It records that three providers entered Tier 2 during the reporting period and that, because the Code does not give new entrants additional time for implementation dates that have already passed, Ofcom is requesting information on their adoption of Code measures over multiple years in the interests of practicality and proportionality. We support that supervisory sequencing and consider that the revised Statement should preserve proportionate supervisory sequencing, without altering the applicable Code expectations or creating a separate tier-transition regime.

Question 2: Do you have any comments on Ofcom's proposed updates to guidance on testing?

Substantial Group supports Ofcom's proposal to streamline the testing section and signpost providers to the Code and Ofcom's Threat Intelligence-led Penetration Testing scheme ("TBEST") handbook. TBEST should remain a voluntary and collaborative assurance mechanism rather than becoming the default testing model for every provider.

The appropriate testing programme will depend on architecture, service criticality, threat exposure and maturity. For a full-fibre provider it may include configuration and access-control assurance, vulnerability assessment, penetration testing of customer and operational systems, privileged-access and supplier-access testing, backup and recovery testing and incident-response exercises. Ofcom should focus on the assurance achieved against material risks rather than assume that a single testing method or point in the equipment lifecycle is appropriate in every case.

That is consistent with the Report. Ofcom found that more than 50% of Tier 1 and 25% of Tier 2 providers appear to find meaningful testing of new equipment before contract award uneconomic or impractical, and said it would examine alternative measures, including testing before deployment into the live environment. This does not dilute the testing obligation; it does support a proportionate approach to how assurance is obtained.

Where testing is required through an assessment notice, operational safety should form part of the proportionality assessment. Annex 7 recognises that mandated testing may use techniques capable of causing a security compromise, loss or property damage. Testing on production network or management systems should therefore be scoped with suitable authorisation, maintenance windows where appropriate, rollback arrangements and customer-impact controls.

² [Ofcom security report for the period October 2024 to October 2025 – GOV.UK](#)

Question 3: Do you have any comments about Ofcom's proposed changes to security incident reporting thresholds and criteria?

Substantial Group supports Ofcom's objective of improving the consistency and usefulness of incident reporting. The existing fixed-network availability thresholds are substantially retained, which provides useful continuity for providers that have embedded them into incident-management processes. There are, however, a number of proposed and inherited provisions where greater precision would materially improve implementation.

Substantial Group has no material comments on the proposed clarification of section 105J user-contact obligations or on the mobile-specific changes, except where mobile reporting requirements may interact with fixed backhaul or wholesale services. Those issues are addressed below.

Critical severity threshold

Ofcom proposes to reduce the critical severity threshold from 3 million to 1.5 million user-hours. This matters for large fixed providers Ofcom proposes to expect an initial notification for a critical incident as soon as possible and usually within three hours, followed by a completed report within 72 hours. An outage affecting 100,000 customers for 15 hours is exactly 1.5 million user-hours, which also illustrates why the boundary wording needs to be exact.

The Consultation explains the 1.5 million figure by reference to Tier 2 Mobile Virtual Network Operator ("MVNO") subscriber bases of between 1.5 million and 5 million. That may be relevant to mobile reporting, but it does not by itself demonstrate that 1.5 million user-hours is the right cross-provider boundary between major and critical incidents for fixed MSNs. Ofcom also states that the change should not result in material costs to communications providers.

Before adopting the lower threshold, Ofcom should explain the fixed-network evidence supporting it, including the number of historical fixed incidents that would have moved from major to critical and the likely operational effect of the three hour process. If the lower threshold is retained, the final Statement should preserve Annex 7's sensible limitation of the initial notification to acknowledgement of the incident, its nature and other information readily available at that stage.

The drafting should also be internally consistent. Paragraph 5.28 refers to incidents that 'exceed' 1.5 million user-hours whereas Table 5 includes incidents at 1.5 million or more. The current Statement leaves exactly 250,000 user-hours unallocated by describing non-urgent incidents as above that level and non-major incidents as below it; proposed Table 5 instead places exactly 250,000 within both Major and Moderate. The revision should remove, rather than reproduce in another form, that boundary ambiguity.

Significance below the published thresholds

The Consultation also makes clear that the published criteria and thresholds are not a safe harbour: an incident may still be reportable under section 105K if it has a significant effect even though no published threshold is met. We recognise the statutory basis for that position. The practical difficulty is that a provider must still decide, often quickly, when a below threshold fixed network incident is sufficiently significant to report.

Ofcom should provide short worked examples or indicative factors, particularly for business connectivity supporting critical activities, compromise of an important network function with limited immediate customer impact, geographically dispersed effects and wholesale incidents where downstream impact is not yet known. This would make the residual statutory test easier to incorporate into incident-triage procedures without turning the published thresholds into a safe harbour.

Repeat incidents and severe weather

The four-week repeat-incident rule is carried forward from the current Statement rather than introduced by this consultation. Its scope nevertheless remains uncertain. It requires aggregation where incidents recur within four weeks or where separate compromises affect the same services in the same areas over a four-week period. Ofcom should clarify the degree of connection required so that genuinely independent incidents are not aggregated solely because they affect the same service and geography.

The same issue arises with severe weather. The Consultation explains that geographically dispersed outages may be combined where, viewed as a whole, they stem from a common cause. That principle is reasonable. That common cause qualification should be carried through expressly into Annex 7. Paragraph 5.22 of Annex 7 refers more generally to combined interruptions, including geographically dispersed severe-weather outages, without repeating the common-cause wording used in the consultation. To avoid the operative guidance being read more broadly than Ofcom's stated policy, Annex 7 should make clear that aggregation in these circumstances is required where the interruptions form part of the same security compromise or stem from a common cause. In a fibre network, however, one storm can produce independent fibre cuts, power failures, flooding and third-party repair damage across separate network segments. Worked fixed-network examples should distinguish one common-cause security compromise from several operationally independent incidents occurring during the same weather event. Providers should also be able to update their classification as causation becomes clearer without being treated as non-compliant for a reasonable initial assessment based on the information then available.

Third-party and wholesale information

We agree that statutory reporting responsibility cannot be outsourced. We also welcome Annex 7's recognition that wholesale providers may have little or no visibility of downstream end customer numbers, are not expected to redesign monitoring systems solely to obtain that information, and that the proposed approach may result in duplicate reporting. The Report underlines the importance of this point: third-party failures remained one of the two predominant causes of resilience incidents and supplier oversight remains an active area of Ofcom supervision.

The final drafting should align those safeguards with Annex 7's expectation that a provider reliant on a third party will collect the required information. In our view, the appropriate standard is information held by the provider or reasonably obtainable through the contractual and operational arrangements that providers are expected to maintain under the security framework. It should not follow that a provider is non-compliant because a supplier's confirmed root cause or downstream impact is unavailable during the initial reporting period. The form should permit estimates and unknowns, followed by updates as information is confirmed.

Where a common upstream event affects several providers, Ofcom should allow reports to cross-reference a shared incident or third-party reference. Each provider would remain

responsible for reporting the effect on its own PECN/PECS, but common root-cause evidence and technical narratives should not need to be recreated by every affected party.

Counting affected customers across broadband, voice, wholesale and leased lines

The Consultation states that on fixed networks customer connections are ‘essentially static and therefore known’. That is too broad for fixed wholesale and business-connectivity models. A retail access provider may know its active line base, but a wholesale fibre provider may not know downstream retail users, and a leased-line service may support one contracting enterprise, many sites, multiple circuits or a much larger population of employees and end users. Annex 8 itself recognises this information asymmetry.

The proposed guidance also asks providers to give affected-customer numbers for every service associated with an incident, including voice and data. That is useful for understanding service impact, but the Statement should distinguish service impact reporting from the customer count used to determine a quantitative threshold or user hours severity.

For example, if the same residential customer loses broadband and a digital voice service as a consequence of one access network incident, Ofcom should state whether that customer is counted once for threshold and user hours purposes while the two affected services are reported separately. Without that distinction, providers could reach different severity classifications for the same underlying event.

The guidance should also preserve the distinction already recognised in Annex 8 between a service a provider sells and an additional Over-The-Top (“OTT”) service used by its customer without the provider’s direct involvement. This is particularly important for digital voice and emergency access. Where a Substantial Group company provides the voice service directly, its impact should be reported accordingly; where it provides only the underlying broadband connection for an independent OTT service, the reporting obligation should not extend to a service it does not provide or monitor.

Pre-positioning

The substantive pre-positioning test is not new. The current Statement already treats unauthorised access that puts a person in a position to bring about a further significant compromise as reportable even where a successful follow-on attack is unlikely, and Annex 7 carries that approach forward. The practical question is the technical connection between the compromised asset and the PECN/PECS.

The Report presents the case for Ofcom’s use of clear examples. It records nine cyber-security notifications, four of which Ofcom considered likely to fall below its mandatory reporting thresholds, and says that Ofcom intends to clarify expectations for cyber incidents, including pre-positioning. Clearer examples will help providers apply the statutory test consistently while continuing to report conservatively where the facts are uncertain. For a fixed network, useful examples would distinguish compromise of an isolated corporate application from compromise of identity or privileged-access systems, network jump hosts, Operations Support Systems (“OSS”), Network Management Systems (“NMS”), provisioning platforms, routing or authentication systems.

Qualitative criteria: Government reporting and media coverage

Two qualitative criteria are carried forward from the current Statement: incidents reported to other Government agencies or departments, and incidents known to have been reported in

local, national or trade media. Under the current Statement those media reports make an incident reportable, but only national mainstream media coverage is an 'urgent' criterion. Proposed paragraph 5.28 places local, national or trade media coverage within the 'critical' criteria as well as separately retaining national mainstream media coverage. Because paragraph 5.26 links a critical incident to the three-hour notification process, the proposed wording appears to widen the three-hour category.

The consultation does not separately identify or explain that change. Paragraph 3.47 describes the move from 'urgent/non-urgent/non-major' to 'critical/major/moderate' as a terminology change that does not affect reporting timeframes, while separately identifying the user-hours reduction as a substantive change to critical reporting. The media wording in paragraph 5.28 may therefore be a drafting artefact. Ofcom should either remove the local/national/trade-media limb from paragraph 5.28 or explain the intended policy change and assess its impact. Media visibility alone is a poor proxy for severity during the first hours of an incident.

The concern is not whether media reporting is accurate. It is that media visibility is not, without more, a reliable measure of the statutory significance or urgency of a security compromise, particularly before technical diagnosis is complete.

The inherited Government-reporting criterion also needs clarification. For the avoidance of doubt, Ofcom should confirm whether 'reported' in this context means a formal incident notification, as distinct from general threat-intelligence sharing or technical engagement with NCSC. Clearer guidance would support early engagement with NCSC without creating uncertainty about the scope of the reporting criterion. Where another public authority already holds relevant information, Ofcom should permit it to be incorporated by reference where lawful and practicable.

Mobile-specific criteria and fixed backhaul

The new cell-site and rural mobile criteria, Annex 10 postcode dataset and Annex 11 Radio Access Network ("RAN") data standard are directed at Mobile Network Operator ("MNO") reporting. They should not create an indirect obligation on a fixed provider merely because it supplies fibre backhaul or leased-line connectivity to an MNO. A fixed provider should report the affected circuits, assets and service impacts that it holds; RAN cell identifiers, coverage and mapping information should be provided by the MNO that operates the RAN.

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

Substantial Group supports the move to a more structured 72-hour form and closer alignment between that form and the monthly bulk-reporting template. The templates should improve consistency, provided they are designed around the information that can reasonably be established during a live incident.

Annex 8 already recognises that exact customer numbers may not be available, that reasonable estimates may be required and that wholesale providers are not expected to redesign monitoring systems to obtain downstream information. Those principles should be reflected in the form fields and validation rules. In particular, the templates should distinguish:

- the provider's role in the affected service – retail, wholesale / network, managed service or mixed;
- unique affected customers from affected services, lines, circuits or sites;

- the basis of the impact figure – actual, estimated, modelled, unknown or not held;
- direct voice or emergency-service impact from impact to an underlying connectivity service;
- third-party information that is confirmed, suspected or still awaited;
- separate timestamps for occurrence or commencement, detection or discovery, and the point at which the provider became aware of the reportable security compromise; and
- whether the incident has been notified to another relevant public authority and, where useful, the corresponding reference.

The timestamp distinction matters. Annex 8 labels field 3 'Date and time of occurrence' but asks for when the compromise occurred 'or when first discovered'. Those can be materially different, particularly for a latent cyber compromise. The current Statement asks for the time the compromise commenced, while the reporting timeframes in Annex 7 run from the provider becoming aware of the incident. Separate fields for commencement, where known, discovery and reportability awareness would avoid ambiguity in both incident analysis and the reporting clock.

Cross-regime incident reporting and regulatory coordination

A single incident can engage more than one reporting route. For a Substantial Group company providing PECS, the clearest overlap is between section 105K reporting to Ofcom and, where the same facts also constitute a reportable personal-data breach under the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR"), notification to the ICO. Engagement with NCSC may also be appropriate. One notification cannot displace a statutory duty owed to another authority, but that does not require the same factual account to be recreated several times.

Ofcom should therefore work with the ICO, NCSC and DSIT on a common set of core incident fields, a shared incident reference and a process for incorporating information already supplied to another authority by cross-reference or attachment. This would build on the information-sharing gateways already described in section 7 of the Statement. Regulator-to-regulator sharing should be used where lawful and subject to appropriate confidentiality safeguards.

The Government's Cyber Security and Resilience proposals similarly emphasise streamlined incident reporting and information sharing. There is also a practical alignment in timing: PECR breach notifications are generally due to the ICO within 72 hours of awareness of the essential facts, while Ofcom's proposed guidance expects the completed incident report within 72 hours. A common factual core would reduce duplication while leaving each authority free to require the additional information needed for its own statutory functions.

Mobile-specific fields, including Global Cell Identifiers, should be conditional so that fixed-only providers are not required to populate or source RAN information they do not hold.

For monthly bulk reporting, Ofcom should publish a stable, version-controlled schema with a data dictionary, validation rules and a clear correction and resubmission process. An incident already reported through the 72-hour process should be capable of being cross-referenced rather than manually re-entered as a duplicate record.

Secure submission also warrants strengthening. Annex 7 proposes email as the default channel for incident reports, with a secure environment available on request. Reports can contain network topology, vulnerable assets, attack paths, supplier dependencies and

information relating to Network Oversight Functions (“NOF”) and Security Critical Functions (“SCF”). Ofcom should provide a standing secure submission route and make it the default for defined categories of sensitive cyber and network–security information rather than requiring a provider to request a secure environment during an incident.

Implementation

The revised Statement should allow a short transition for process and template changes. When the current regime was introduced, Ofcom said that providers needing to adjust internal processes to meet its new guidance should do so within a reasonable period after publication of the final Statement. The same principle should apply here. We suggest at least three months for changes to triage rules, procedures and training, with a test submission facility for the 72-hour and bulk templates and a longer period where systems integration or automation is required. Ofcom should specify a clear effective date for the revised processes and templates and provide transitional guidance for incidents already open at that date. Any transition should be without prejudice to providers’ underlying statutory duties under section 105K.

Question 5: For MNOs: Do you have any comments about the requirement to provide Ofcom with a list of RAN cells for purposes of mapping incidents and their impact?

This question is directed to MNOs and is not applicable to Substantial Group’s fixed full fibre network businesses. Annex 11 is expressly a standard for MNOs providing monthly RAN information. In those cases where a Substantial Group company supplies fixed backhaul or leased line connectivity to an MNO, it can report affected circuits, assets and service information within its control, but should not be expected to create or maintain the MNO’s RAN cell mapping data.

3. Conclusion

Substantial Group supports Ofcom’s proposed update to the section 105Y Statement. The Report shows a regime that is maturing and also identifies practical issues around supplier oversight, testing and cyber incident classification. The revised Statement presents an opportunity to resolve those issues and improve the quality of reporting without adding process that does not improve security outcomes.

In our view, the final Statement should be precise enough to be applied reliably during a live incident and proportionate enough to keep operational teams focused on containment, restoration and customer protection. The same principle should apply across reporting regimes: common core incident information and practical cross referencing between Ofcom and other relevant public authorities would preserve statutory accountability while reducing duplication.

If Ofcom would find it helpful, we would welcome a discussion of the points raised in Substantial Group’s response to the Consultation.