

**Openreach's response to:
Ofcom's procedural guidance
consultation dated 12 May
2026**

August 2026

Openreach's response to Ofcom's consultation: Ofcom's draft general statement of policy under s105Y of the Communications Act 2003 (Ofcom's procedural guidance)

Table of contents

Introduction.....	3
Openreach's comments on Ofcom's proposals.....	3
Question 1: Proposed updates to guidance on compliance monitoring.....	5
Information gathering – managing the impact on stakeholders.....	5
Powers to assess compliance - Assessments and assessment notices (sections 105N -105Q).....	6
Question 2: Proposed updates to guidance on testing.....	8
Expanded powers under section 105N of the 2003 Act to monitor compliance with the security duties.....	8
Question 3: Proposed changes to security incident reporting thresholds and criteria.....	9
a) Section 105J to inform users of risk of security compromise.....	9
b) Section 105K Security compromise reporting to Ofcom.....	10
Question 4: Proposed changes to reporting templates	12
Structure, clarity and ease-of-use of the reporting form.....	12
Question 5 (for MNOs): list of RAN cell data	12

Introduction

On 12 May 2026, Ofcom published its consultation document entitled *"Consultation on Ofcom's draft general statement of policy under s105Y of the Communications Act 2003 (Ofcom's procedural guidance)"*.

This response is provided by Openreach Limited - a wholly owned subsidiary of BT Group plc.

Openreach's comments on Ofcom's proposals

1. Openreach welcomes the opportunity to comment on Ofcom's draft General Statement of Policy under section 105Y of the Communications Act 2003. This response is submitted in our capacity as a provider of public electronic communications networks (PECNs) and Tier 1 provider.
2. While we recognise the value of clear procedural expectations within the Telecommunications security regime, we set out below a number of observations and suggested refinements to help ensure the guidance is clear, consistent and practical to implement.
3. This response reflects Openreach's experience in implementing the Telecommunications Security Act framework and is focused on areas most relevant to operational delivery and compliance.
4. In common with BT's response, the Openreach response focuses on three themes:
 - a. **Clarity** – the reporting framework should be capable of being applied consistently by the operational teams who make reporting decisions, often at pace and while an incident is still unfolding. Several of the current requirements can only be applied by cross-referring between multiple overlapping thresholds, categories and timelines, which makes consistent, real-time decision-making difficult.
 - b. **Proportionality** – new requirements should be operationally workable, and their benefits should be weighed against their cost. Responding to Ofcom's information-gathering already carries a material burden
 - c. **Regulatory value** – reporting obligations should be targeted at the information that delivers the greatest regulatory insight. Where the reporting boundary is drawn too broadly, a higher volume of lower-significance notifications risks diluting Ofcom's visibility of the incidents that matter most.
5. Where additional reporting or data requirements are proposed, Openreach also considers that each should be clearly linked to a specific regulatory objective and supported by a proportionate assessment of its costs and benefits.

6. Our principal concern is that the consultation assesses each proposed change in isolation rather than in the round. Taken together, the proposals would require providers to supply more information, more frequently and in greater detail, and the consultation does not yet demonstrate that this would materially improve Ofcom's ability to identify, assess or respond to the incidents presenting the greatest risk.
7. This is inconsistent with Ofcom's Growth Duty, which recognises that:
*"a disproportionate approach, conversely, goes far beyond what is necessary and can stifle productivity as it ties up business and regulator's time and resources that could be more productively deployed elsewhere."*¹
8. Openreach therefore encourages Ofcom to test the cumulative impact of the proposals and, where the regulatory benefit is not clearly established, to refine them so that the final framework remains both effective and proportionate. In that spirit, BT's response includes a practical decision tree to help make the regime workable in practice.
9. The remainder of this document sets out Openreach's responses to Ofcom's specific questions.

¹ See Driver 5: Efficiency and Productivity in [Growth Duty: Statutory Guidance - Refresh](#), 21 May 2024, Department for Business and Trade

Consultation questions

Question 1: Proposed updates to guidance on compliance monitoring

Information gathering – managing the impact on stakeholders

Openreach takes its obligations under the Telecommunications Security Act 2021 (TSA) very seriously and recognises the important role that information requests play in enabling Ofcom to assess compliance with the statutory security duties and associated regulatory requirements. We work closely with Ofcom's Information Registry Team and greatly value the coordination and engagement undertaken with stakeholders.

Given the breadth and complexity of the information Openreach provides to support Ofcom's monitoring and compliance with the TSA, we support Ofcom's proposal to amend the estimated cycle for TSA related information requests, extending it from nine months to twelve months in the updated Statement of Policy. We recognise that the timing and frequency of requests may need to vary in response to emerging risks, significant security compromises, regulatory priorities or other relevant developments.

We note that Ofcom has previously established internal governance arrangements to ensure that information requests are necessary, proportionate and appropriately targeted. This is particularly important in the context of the TSA, where requests frequently relate to complex technical, operational, governance and risk management controls spanning multiple business units and stakeholders. Effective scrutiny prior to issue helps ensure that requests are clearly defined, proportionate to the regulatory objective being pursued. In turn, this enables Openreach to focus resources on providing accurate, complete and timely responses, improving the overall effectiveness and efficiency of the information gathering process.

We also consider it important that Ofcom continues its established practice of sharing draft section 135 notices with providers before they are finalised. In the TSA context, this engagement provides an opportunity to identify potential issues relating to scope, proportionality, feasibility, terminology and timescales before a formal notice is issued. This is particularly beneficial where requests relate to highly technical security controls, complex network architectures or information held across multiple functions.

Early dialogue between Ofcom and Openreach provides an opportunity to discuss the scope, purpose and intended use of information requests, helping to identify potential issues, clarify requirements and align expectations before formal requests are issued. This enables stakeholders to better understand the context of requests, improve the quality and consistency of responses, and reduce the risk of unnecessary burden or duplication. In our experience, regular engagement promotes a more collaborative and

efficient information gathering process, ultimately benefiting both Ofcom and stakeholders by supporting the provision of accurate, relevant and timely information.

Powers to assess compliance - Assessments and assessment notices (sections 105N -105Q)

Openreach recognises Ofcom's view that, in some circumstances, assessment notices may provide a more proportionate means of assessing compliance than extensive written information requests. We agree that direct engagement can be an effective supervisory tool. However, the consultation provides limited detail on how assessment notices would operate in practice, particularly the circumstances in which Ofcom would choose to use an assessment notice rather than an information notice, and the factors that would inform that decision.

Assessment Notice

Openreach does not agree that assessment notices should be presumed to be less operationally burdensome than information notices (consultation paragraph 3.14). The existing information notice process provides important governance and quality assurance benefits. Responses to TSA section 135 notices typically require input from multiple technical, operational, security, legal and compliance stakeholders. The process enables providers to validate information, reconcile differing inputs, review supporting evidence, and ensure that responses accurately reflect organisational practice.

In practice, many of these activities would still be required to support an assessment notice. Providers would need to identify relevant stakeholders, coordinate input across multiple teams, review documentation, prepare participants for interviews, facilitate access to systems, respond to follow-up queries, and review records of discussions. Assessment notices may therefore transfer the burden from preparing written responses to supporting and managing assessment activity rather than reducing it.

Any assessment of proportionality should take account of the total resource effort required to prepare for, participate in, and follow up on assessments, rather than focusing solely on any reduction in written submissions.

Accuracy and quality assurance

Openreach is concerned that interviews and assessments conducted over a relatively short period may increase the risk of incomplete, inconsistent, or misunderstood information being provided, particularly where questions relate to complex technical environments, multiple business units, or specialist subject matter. This could reduce the accuracy of information available to Ofcom and increase the need for subsequent clarification.

To support accurate and reliable information gathering, providers should be given sufficient notice of the topics to be discussed, appropriate opportunities to identify relevant subject matter experts, and the ability to provide supplementary written

evidence or clarification following interviews where necessary. This would enable Ofcom to benefit from direct engagement while retaining the quality assurance advantages associated with the current information notice process.

Transparency and safeguard

To be effective, assessment notices should form part of a coherent and streamlined compliance framework, supported by clear guidance on when they will be used and how they will interact with other information-gathering powers. The draft revised statement of policy proposes to make greater and more routine use of assessment notices as a standard supervisory tool (paragraphs 3.13 to 3.14). That expansion of Ofcom's powers of entry, inspection and compelled interview under section 105O is not matched by any corresponding procedural safeguards in the statement.

Openreach therefore encourages Ofcom to provide a clearer explanation of the factors it will consider when deciding whether to use an assessment notice or an information notice.

For the power of entry, the statement commits only to having regard to the Home Office Code of Practice on Powers of Entry where relevant (paragraph 3.43) and to annual reporting of the occasions on which premises have been entered (paragraph 3.44). We recognise that the Home Office Code already supplies many of the safeguards. However, the Code applies to entry only and does not touch the power to require persons to be made available for interview under section 105O(2)(c).

Therefore, we would expect Ofcom to establish clear criteria governing the use of interviews, together with appropriate safeguards for participants. These should include: individual's rights and obligations; transparency regarding the purpose and scope of discussions; how information will be recorded and used; how any record of the interview will be retained and made available to the individual and the provider; how the privilege against self-incrimination applies to interviews conducted under an assessment notice; the extent to which an individual may be required to answer questions as opposed to providing existing factual or documentary information; and any other protections to ensure interviews are conducted in a fair, consistent and proportionate manner.

Setting out these safeguards in the statement would provide providers and individuals with clarity and predictability and support the fair and proportionate exercise of the section 105O powers.

Cost recovery

While Ofcom states that it may be appropriate and proportionate for the costs of third-party assessments to be borne by the regulated provider², it would be helpful to understand in greater detail the circumstances in which costs may be passed on to Openreach and the basis on which those costs would be determined. Further clarity on the expected scope of assessments, the approach to cost allocation, and any

² Telecommunications (Security) Act 2021 amendments to the Communications Act 2003 section 105N(2)(b).

safeguards to ensure costs remain proportionate would assist stakeholders in evaluating the proposal.

Question 2: Proposed updates to guidance on testing

Expanded powers under section 105N of the 2003 Act to monitor compliance with the security duties

Openreach shares the Government's and Ofcom's objective of improving the security and resilience of UK communications networks and remains committed to meeting all applicable obligations under the telecommunications security framework.

Openreach products and services are subject to established independent IT health checking, testing and assurance processes. We therefore support an approach that takes account of existing testing and assurance activities when considering whether additional testing is necessary. Any additional testing required by Ofcom should be targeted, risk-based and focused on addressing specific assurance gaps, rather than duplicating existing controls and assessments.

To provide greater certainty for providers, Ofcom should set out clearer criteria for when additional testing may be required, the factors that would trigger such testing, the frequency with which providers might reasonably expect to be subject to it, and the steps that will be taken to avoid duplication with existing assurance frameworks and industry-led testing activities.

We also note that section 105O(4) permits Ofcom to require realistic security testing that may involve a degree of operational risk. However, neither the legislation nor the draft guidance clearly explains the circumstances in which such testing would be expected to take place in live production environments, pre-production environments, or segregated test environments. Greater clarity on Ofcom's expectations would help providers understand when testing of live systems may be considered necessary, proportionate and appropriate, and how associated operational risks should be managed.

Question 3: Proposed changes to security incident reporting thresholds and criteria

Openreach follows the BT Group plc security and resilience incident reporting framework and reports all significant security and resilience incidents that meet the relevant criteria and thresholds set out in Ofcom's 2022 guidance.

a) Section 105J to inform users of risk of security compromise

Openreach supports the objective of ensuring users are informed where there is a genuine risk of harm arising from a security compromise. However, the draft guidance would benefit from greater clarity on when the duty under section 105J is triggered and how it should be applied in practice.

In particular, the guidance does not adequately reflect the wholesale-retail structure of the telecommunications market. As a wholesale provider, Openreach's relationship is primarily with Communications Providers (CPs), rather than end users. The guidance should clarify how notification responsibilities are expected to be allocated between wholesale providers and CPs, including who should communicate with end users and how consistent messaging should be achieved across the supply chain.

Openreach is also concerned that the guidance does not provide a sufficiently clear and objective trigger for user notifications. While it identifies factors that may be relevant to assessing whether a "significant risk of a security compromise" exists, it does not explain when that threshold is met in practice. Unlike the proposed guidance for section 105K incident reporting, no equivalent thresholds, criteria or examples are provided. This creates a risk of inconsistent interpretation across industry and uncertainty as to Ofcom's expectations.

Further clarity is particularly important given that the section 105J threshold of a "significant risk" appears materially different from the broader "increased risk" concepts used elsewhere in the telecommunications code of practice³. Openreach therefore encourages Ofcom to provide additional guidance, including practical examples, to help providers determine when user notifications are expected and the factors that should be taken into account when assessing risk.

Finally, the guidance should recognise that providers may require time to investigate and remediate vulnerabilities before information can be disclosed safely. Flexibility is therefore needed to ensure that notifications support user protection without inadvertently increasing cyber-security risks or creating new compliance obligations beyond those set out in the Act, Regulations and Code of Practice.

³ [Telecommunications Security Code of Practice 2026 \(version 1.1\) - GOV.UK](#)

b) Section 105K Security compromise reporting to Ofcom

Pre-positioning attacks

Openreach supports Ofcom's recognition of the threat posed by pre-positioning⁴ attacks and agrees that providers should report incidents where an attacker has obtained a foothold that could reasonably enable a subsequent security compromise with significant operational impact.

In practice, security teams routinely detect and contain a wide range of attempted and successful intrusions of varying severity, many of which are isolated before they present a realistic risk to network operations or customers

Openreach, via BT Group plc, provides Ofcom with regular cyber threat intelligence on an informal basis through its monthly cyber threat levels report.

Openreach understands that the proposed changes are intended to formalise the circumstances in which information should be provided to Ofcom. We would welcome further engagement with Ofcom to confirm that interpretation and to provide clarity on how "pre-positioning" will be defined, including how it will be distinguished from routine operational activity or vulnerabilities that are being actively managed.

Reporting of security incidents

Paragraph 5.18 states that incidents having a "significant effect" remain reportable under section 105K, but no explanation is provided as to how providers should assess significance in these circumstances. This introduces considerable uncertainty and risks inconsistent interpretation between providers. Ofcom should clearly define the criteria that trigger reporting where the stated thresholds have not been met and provide clarity on the circumstances in which an incident is expected to be reported under section 105K.

Media coverage

Openreach seeks clarification on the proposed criterion requiring providers to report security compromises that are known to be the subject of media (local, national or trade news sources)⁵. Whilst Openreach understands Ofcom's interest in significant incidents attracting public attention, it is unclear how providers are expected to comply with this requirement in practice.

The draft guidance does not specify the extent to which providers are expected to monitor media sources, what constitutes awareness of media reporting, or whether providers are expected to implement dedicated monitoring arrangements to identify relevant coverage within the 3 hour reporting timeframe.

⁴ See draft guidance Paragraph 5.15

⁵ See draft guidance paragraphs 5.19 and 5.28

Openreach already operates a national mainstream media monitoring process based on a defined list of publications. As currently drafted, the criterion could be interpreted as requiring proactive monitoring of a broad and fragmented media landscape, particularly local media, which may be difficult to monitor comprehensively. This creates uncertainty as to the scope of providers' obligations and monitoring of local media should not in itself determine whether an incident is reportable.

Openreach is also concerned that the criterion appears to be based on the existence of media coverage rather than the security significance or impact of the incident itself. This could result in similar incidents being treated differently depending on the level of public or media interest they attract.

Linking of incidents

Openreach seeks further clarification regarding the expectation that providers combine interruptions⁶ when assessing whether reporting thresholds have been met. While Openreach understands the rationale for capturing the cumulative impact of related incidents, it is not always clear how providers should determine whether multiple service interruptions form part of the same security compromise or should be treated as separate events. This is conducted through post event analysis.

In practice, correlating and aggregating multiple incidents across different geographies, network components and time periods may require significant resource, particularly during major service-impacting events when operational teams are prioritising restoration activities. As drafted, there is a risk that providers devote resources to incident correlation and threshold calculations at a time when customer restoration is the primary objective.

We therefore ask Ofcom to confirm that, where operational resources are at capacity during an incident, reporting on combined interruptions is expected to be undertaken as part of a post-event analysis rather than in real time.

Severe weather

The guidance refers to "severe weather" but does not define the term, making it unclear when the aggregation requirement would apply. Openreach encourages Ofcom to adopt objective criteria, such as named storms or specified Met Office warning categories, to provide greater certainty and promote consistent reporting.

Quantitative reporting severities

Openreach seeks clarification on the intended scope of the proposed incident severity classifications of "critical", "major" and "moderate".⁷ While the consultation⁸ appears to introduce these categories as a general reporting framework for security compromises under section 105K, the draft guidance associated thresholds and metrics appear to be derived from mobile network reporting, including references to affected cell sites. It is

⁶ See consultation paragraph 3.46 and draft guidance paragraph 5.22.

⁷ See draft guidance paragraph 5.25, Table 5

⁸ See consultation paragraph 3.47

therefore unclear whether the revised classification is intended to apply equally to all PECN/PECS providers or whether certain elements are directed primarily at mobile operators and MVNOs.

As a fixed network provider, Openreach does not operate mobile cell sites and therefore it is unclear how these criteria should be interpreted in the context of Openreach's networks and services. Openreach would welcome clarification on how the framework should be applied by fixed network providers and whether alternative criteria are envisaged where mobile-specific measures are not applicable.

Question 4: Proposed changes to reporting templates

Structure, clarity and ease-of-use of the reporting form.

Openreach supports the use of a standardised template where they improve consistency, comparability and data quality.

72 hour reporting: Openreach welcomes Ofcom's recognition that initial incident notifications may need to be submitted before all relevant information is available, and that reports can be updated as further information emerges. This reflects the practical realities of incident management and investigation, where the full scope, cause and impact of an incident may not be known at the point of initial notification.

Openreach also notes that the proposed reporting template differs in some respects from the incident notification template currently used by Openreach, including the removal of fields such as "Summary of actions taken" and "3rd Party Damage". We would welcome clarification on the rationale for these changes and how the revised template is intended to align with existing reporting processes, to support efficient and consistent incident reporting.

Question 5 (for MNOs): list of RAN cell data

Openreach has no comments in relation to MNOs incidents.