

Question	Your response
to our guidance on compliance monitoring?	
Question 2: Do you have any comments on our proposed updates to our guidance on testing?	Confidential? – N Please see below comments
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?	Confidential? – N Please see below comments
Question 4: Do you have any comments about the proposed changes to our reporting templates?	Confidential? – N Please see below comments
Question 5: (for MNOs): 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?	Confidential? – N/A

Please tell us how you came across this consultation: **Found it on Ofcom's website**

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

Response from the Internet Service Providers Association (ISPA)

Contact: ispa@policy.org.uk

About ISPA

1. The Internet Services Providers' Association is the trade association for the Internet industry in the UK. Our membership consists of 150 ISPs and network operators rolling out and operating networks on a national and local scale utilising a variety of technologies.
2. Our members range in size and sit across different tiers under the Telecommunications Security Act. The proposals in this consultation therefore affect our membership to different degrees. This breadth informs our response, and our response reflects the need for a regime that is proportionate, predictable and clear for providers of every size and tier.

About our response

3. ISPA welcomes the opportunity to respond to Ofcom's consultation on proposed updates to its General Statement of Policy under section 105Y of the Communications Act 2003.
1. Security and resilience has long been a priority for the internet industry – through investment, design, regulation and best practice – and our members play a critical role in keeping the country and our economy connected and secure.
2. We welcome Ofcom's intention to keep its guidance current after three years under the security framework, and the intention to further strengthen the resilience of the UK's telecommunications networks and keep the regulatory framework effective.
3. However, ISPA highlights that the framework must remain proportionate, predictable and clear. Proportionality and clarity are crucial for investment and the predictable planning of compliance, but also for security outcomes. Where obligations are disproportionate, they draw operational teams away from maintaining network integrity and responding to the most serious live threats.

4. Taken together, several of the proposals risk increasing the compliance burden on providers — particularly through the more routine use of assessment notices — and generating a greater volume of reporting without a corresponding regulatory benefit. This is most acute in relation to cyber incident reporting, where members need a clear methodology and thresholds rather than a general expectation to report more.
5. ISPA also highlights that Ofcom's supervisory and enforcement powers should be exercised reasonably and predictably, with effort focused where the risk is greatest.
6. Finally, given that the burden of responding to Ofcom's powers — including the cost of assessment notices operating as mini-audits — falls on providers, it is essential that providers are given sufficient notice and clarity to plan and resource their compliance.
7. We welcome the proposed move to an approximately twelve-month information notice cadence, which better reflects the time providers need to comment on draft questions and compile responses. We would welcome an equivalent commitment in relation to assessment notices: specifically, that Ofcom will, where practicable, issue assessment notices in draft for comment before they are finalised and will set out a defined minimum response period and clear scope. This would give providers a predictable basis on which to plan and resource their compliance.
8. As an association representing the fixed sector, our response focuses on the first four consultation questions.

Consultation questions

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

1. While ISPA recognises that some of the proposed changes are intended to be positive, in particular the move from an approximately nine-month to twelve-month information notice cadence, we are concerned that the overall direction of the compliance monitoring changes represents a net increase in regulatory burden.
2. In particular the combination of minor changes to existing information requests, additional and more targeted information requests, and the more routine use of Assessment Notices, which operate in effect as mini-audits

whose cost falls on the provider. This concern is felt most acutely by Tier 1 providers under the TSA definitions.

3. ISPA is also concerned about the impact of Assessment Notices as a potentially burdensome regulatory tool. Members consider they are more appropriately reserved for circumstances where Ofcom has *prima facie* grounds to believe a provider may not be complying with its security duties, rather than being used as a routine information-gathering mechanism, for which there are existing powers through information requests..
4. ISPA does not consider Assessment Notices as less burdensome than Information Notices. ISPA could also highlight that they can be highly intrusive, as they can involve any of interviews, testing, site access, inspection of information and potentially provider-funded costs. For live networks, operational systems and security controls, the burden and risk associated with these activities can be significant, particularly where testing is involved. They also require greater resourcing than Information Notices: an information notice allows a provider time to organise and prepare its response, whereas an assessment notice presents a more immediate and less predictable demand. Finally, Assessment Notices typically require operational personnel to be taken away from their day-to-day duties – the same people responsible for maintaining network integrity and responding to live threats – at short notice.
5. For these reasons, an information notice should be the default first step, with assessment notices used by exception rather than as a matter of routine. Ofcom should take account of provider evidence from existing assurance activity, control monitoring, governance forums, security quality gates and other compliance processes before deciding whether an assessment notice is necessary.
6. Ofcom should provide greater transparency and procedural clarity on the circumstances in which Assessment Notices will be issued, and on the steps that will precede their use, including their intended frequency and scope.
7. More broadly, supervisory and assessment powers should be exercised reasonably and predictably. Where the use of powers is routine, Ofcom should give good notice and clear detail on what will be covered, so that providers can plan and resource their response.

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

1. ISPA is concerned that the draft guidance appears to imply that operators who choose not to participate in Ofcom's TBEST testing programme may face a greater likelihood of receiving Assessment Notices. This risks creating an inappropriate incentive structure that would make TBEST a de facto mandatory requirement.
2. While TBEST may be suitable for some operators, it is not necessarily the most appropriate or proportionate third-party testing regime for every organisation.
3. Ofcom should make clear that participation in TBEST is genuinely voluntary, and that alternative, equivalent assurance approaches will be recognised.
4. ISPA would also highlight that testing can be highly intrusive, and members would welcome greater clarity on the scope of what is being requested in any given instance. Given this and the planning and resource that testing requires, ISPA would suggest that testing is not used as a default position, and that clear guardrails are set out around when and how it will be used.
5. We also request that any mandated testing – particularly testing that could risk causing a security compromise or service disruption – be carefully planned with the provider in advance. Ofcom should provide detail on the objectives, scope, method, timing, safety controls, rollback arrangements and expected operational impact of the testing. This will ensure that the provider can assess risk and ensure the appropriate internal subject matter experts are available.

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?

1. ISPA members have several concerns about the proposed changes, which taken together, risk imposing a significant additional compliance burden while generating an unmanageable increase in the volume of reports submitted to Ofcom.
2. On cyber incident reporting in particular, we are concerned that Ofcom has signalled a clear expectation of greater reporting of cyber incidents without providing an accompanying playbook, thresholds or methodology equivalent to those that exist for resilience outages. Large providers

experience very high volumes of attempted attacks, which are internally triaged by severity, and it is unclear which of these Ofcom expects to be reported or against what parameters.

3. ISPA would highlight that the absence of a threshold for cyber incident reporting, in contrast to the position for resilience incidents, presents a particular difficulty for members. It is operational teams who must manage this reporting in practice, and they would benefit from clear guidance on what is expected to be reported. Without such guidance, members are concerned that the obligation would be difficult to apply consistently.
4. The proposed broad "catch-all" requirement to report all "significant" security incidents, even where they do not meet any specific threshold creates uncertainty and may drive defensive over-reporting.
5. We also note that the new provision on pre-positioning – capturing threats that have not yet had an impact on end-users or the network but could cause future damage – is introduced without any threshold or parameter, leaving providers without a clear basis on which to judge what must be reported.
6. ISPA would also welcome clarity on the treatment of planned maintenance works. Where a provider carries out planned maintenance that may affect a large number of customers, and has given those customers advance notice, ISPA does not consider that this should trigger a requirement to notify Ofcom. Planned works of this kind are, by definition, anticipated, controlled and communicated in advance, and are qualitatively different from the unplanned security and resilience incidents the reporting framework is designed to capture. Treating notified, planned maintenance as reportable would generate volume without regulatory benefit and would draw operational teams away from their core function. ISPA would therefore welcome confirmation that planned maintenance works for which customers have received advance notice do not fall within the incident-reporting obligations, and, if Ofcom takes a different approach, a clear explanation of when and against what threshold such works would need to be reported.
7. ISPA asks that Ofcom clarify what it is seeking to obtain from cyber incident reporting and set out a clear methodology, rather than simply requiring more to be reported.

8. Members are also concerned that the percentage-based customer thresholds disadvantage smaller providers. The 25% customer-base threshold can be triggered by providers with a relatively small customer base even where the absolute number of affected users is low. We therefore advise that this metric is revisited, and also note that the industry has previously raised this concern.
9. The requirement for monthly bulk reporting of all minor incidents could generate substantial administrative effort for limited regulatory benefit. We note that bulk reporting is, in practice, completed by the same operational personnel responsible for fixing the network and responding to security compromises in real time – a point felt particularly acutely on the security-incident side, given the volume of attempted attacks members face. ISPA would therefore suggest that the frequency and volume of bulk reporting be kept proportionate, with clear rules and well-defined categories, so that the reporting burden does not detract from members' core security function.
10. The proposal to treat any incident receiving any form of media coverage as a "critical" incident requiring notification within three hours appears disproportionate. In particular, local or trade media coverage should not automatically make an incident critical regardless of operational thresholds. Media coverage may emerge after the event, and may be incomplete or inaccurate. Moreover, media coverage is not a reliable indicator of the severity or impact of an incident, and this could require operators to make urgent notifications before sufficient facts have been established. Media coverage would be more appropriately treated as a review or escalation factor, rather than an automatic criticality trigger.
11. ISPA would also welcome greater clarity on the terminology used here. It is not clear whether "media coverage" is intended to capture the press, social media, or national mainstream coverage, nor what level of coverage would be relevant. Members would highlight that, were the trigger to extend to social media coverage, this would be disproportionate. ISPA would also note that larger providers may have a dedicated media or communications function monitoring coverage, whereas smaller providers may not, so a media-based trigger risks bearing unevenly across the sector.
12. On the method of notification, ISPA would highlight that the existing framework already permits providers to notify by email. Where the

circumstances allow, members would suggest that notification by email should be sufficient, and that a phone call need not be required as a matter of course – particularly overnight, given that this draws on the same operational teams whose primary responsibility is ensuring the network is not compromised. Where notification by email delivers the same outcome, ISPA would welcome confirmation that it remains an acceptable route.

13. On third-party reporting, where a provider relies on a third party's network the duty to collect and report, members note that information should be qualified by a reasonable/best endeavours standard, recognising that providers need to be able to respond practically. The treatment of resale arrangements (for example, mobile service resale) should also be clarified within the reporting framework.
14. Finally, the scope of wholesale reporting obligations would benefit from greater clarification, as members have raised concerns about duplicative "double reporting." Under the proposals, an underlying wholesale provider may be expected to report an incident affecting its downstream carriers at the same time as those downstream providers report the impact on their own customers. Members note this is difficult to align with what a wholesale provider can observe from its own vantage point on the network, and that carriers already notify one another of relevant incidents through existing incident-management processes. While Ofcom addresses wholesale at paragraph 5.21 – confirming it does not expect providers to alter monitoring or reporting systems to obtain end-customer numbers, with the obligation triggered only where it is "clear to the provider" that thresholds will be exceeded – the consultation does not address whether wholesale-only services supplied exclusively to other carriers constitute "public" electronic communications. ISPA raises this as a useful point for certainty.
15. More broadly, ISPA would welcome further consideration of proportionality here. Members would suggest that a separate report should not be required from both the wholesale and downstream provider where the position can be reported together, particularly as the impact on other providers is, in practice, already captured within the report. ISPA would also highlight that the proposed requirement to securely share information with all wholesale customers within three hours, and again at 72 hours, would place a considerable operational load on providers, and would welcome further discussion of whether this is proportionate to the benefit.

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

16. ISPA welcomes the decision to make the three new reporting template columns – third-party details, global cell IDs, and other notes – optional. This is a positive and proportionate step and should be retained. Members also welcome the broader intention behind the template changes to make reporting more streamlined.