Your response

Questions concerning Ofcom's draft general statement of policy under section 105Y of the Communications Act 2003 (see Annex A5).

Question	Your response
Consultation question 1: Do you have any comments on our proposed approach to compliance monitoring?	*Is this response confidential? N* techUK agrees with Ofcom's assessment that providers' compliance with the new security framework will take considerable time, effort and resource, not least given the scale and complexity of many providers' operations. Our members are grateful to Ofcom for its promise of adopting a collaborative approach to compliance monitoring, as providers undertake this considerable security journey, and we urge Ofcom to begin this engagement as early as possible. techUK agrees with Ofcom's assessment (paragraph 3.6) that security threats will evolve over time, specifically in relation to the pace of technological advancement and innovation in our networks: however, we caution that Ofcom's proposed approach to compliance and regulation, in paragraph 3.10, to "ramp up over time" must be balanced with a risk-based approach that supports network and service innovation, rather than introducing an increasing regulatory burden on UK providers. Ofcom rightly recognises that collecting information about the wide range of security duties and measures covered by any regulations and codes of practice is a new exercise for both the regulator and providers, and techUK members are supportive of Ofcom's proposal to issue draft s135 information notices to providers for comment before finalising them. We recommend that Ofcom considers the significant reporting and

compliance burden on providers as it sets timescales for comment and feedback, as even our largest members do not have unlimited resources to dedicate to these efforts.

On timing, in our consultation response to DCMS[1], techUK has strongly encouraged government to align Tier 1 deadlines to the same timeframe as Tier 2 providers: guidance measures 1.01-7.07 for Tier 1 and 2 providers by 31 March 2025, guidance measures 8.01-11.06 for new contracts should be implemented by Tier 1 and 2 by 31 March 2025, and all contracts by 31 March 2027. Guidance measures 12.01-18.22 should be implemented by Tier 1 and 2 providers by 31 March 2027, and guidance measures 19.01-23.07 should be implemented by Tier 1 and 2 providers by 31 March 2028.

To address techUK member concerns about the volume of information requests and reporting providers will need to deliver to Ofcom, aligning the implementation timescales would ease the administrative and regulatory burden on providers, as well as Ofcom itself (as the regulator sets out its objective of the monitoring process is to "gather information about the implementation of each of the measures in the Code… well in advance of these dates wherever possible").[2] We question whether getting progress updates through formal s.135 (which carry the risk of enforcement and are therefore a very involved exercise) in advance of the deadlines is the best use of time for both Ofcom and providers. This is especially true for those in Tier 2 who, under current proposals, have longer implementation timelines.

We are somewhat concerned that Ofcom may have underestimated the level of evidence and documentation it may receive in response to the information requests it will be issuing. As DCMS have indicated that there are 11 Tier 1 providers (seven fixed, four mobile) and we estimate they may be in the tens of Tier 2

[1] https://www.gov.uk/government/consultations/proposal-for-new-telecoms-security-regulations-and-code-of-practice

[2] Paragraph 3.23 – Annex A5

	providers, we question whether the proposed rolling monitoring programme makes sense. While we strongly support the use of draft information requests, we are concerned at the level of detail that may be requested in information requests, particularly as many of the topics will be sensitive in nature. Having Ofcom retaining such information creates an attractive central point of information for potential threat actors. While we understand that Ofcom is proposing to use a secure system called ROSA, providers would welcome further detail of this system and the security measures that Ofcom will be putting in place at its organisational level.
Consultation question 2: Do you have any comments on our proposed approach to testing?	*Is this response confidential? N* Ofcom proposes that it will continue to run its voluntary red-team style, penetration testing (TBEST) alongside its expanded powers to provide assurance that a provider is complying with (or has complied with) the security duties in sections 105A to 105D, 105J and 105K. techUK welcomes Ofcom's assurance that it aims for a collaborative and open approach with industry throughout its draft statement of policy, and urges the regulator to fully commit to this collaboration, in areas like testing, as the regulation commences. On TBEST itself, some members have raised concerns that the regime is based on CBEST, which was built as an intelligence security testing regime for financial services. There is no information within the guidance as how knowledge built upon a financial services regime is relevant to a testing regime for telecoms, and there is a lack of transparency on this issue, although we note the historical industry engagement that took place when TBEST was initiated. We also note that the established model of CBEST was used as it was a proven assessment approach on how to enable intelligence-led red teaming on live critical systems to assess their resilience to real world cyber threat actors. That approach was adapted for the telecommunications sector to create TBEST the historical industry engagement, noted above, that considered the

specific threats to the sector and telecommunications operational environment, to ensure that the assessment model was viable. This was then proven through execution of TBEST assessments.

Other members with experience of TBEST exercises, have informed techUK that the skill in running a useful TBEST comes from making a good choice of pen test partner, with relevant telecoms experience. Therefore, a good outcome for a network or service is possible.

Ultimately, it is unclear in the guidance how providers can verify that their pen testing partner has the relevant telecoms experience before employing them to undertake a test. Furthermore, members seek further clarification from Ofcom on how using TBEST in its proposed approach will test against the full range of security requirements as set out in the draft code of practice, such as supply chain security and SIM cards. techUK recommends that Ofcom addresses these concerns as a matter of urgency.

techUK has also received feedback on Ofcom's proposed approach to testing from some members that questions why TBEST appears as the only mechanism that can be used for testing. There is also the 3GPP SCAS Reference[3], and the GSMA NESAS framework[4] which is assurance for equipment, and that goes through recognised test labs. Many providers will already have their own internal and external pen testing regimes. Indeed, global providers may also need to comply with penetration testing requirements from other countries, and may operate such testing at a global scale, and it would be disproportionate to require them to duplicate this with a UK specific test. There is a good industry testing that can also be drawn upon, in a complementary package of testing.

Some techUK members, drawn from across the telecoms ecosystem, have questions whether the proposed approach to testing is

[3] 3GPP SCAS Reference 33.511-33.527 - https://www.3gpp.org/DynaReport/33-series.htm

[4] GSMA NESAS - https://www.gsma.com/security/network-equipment-security-assurance-scheme/

	proportionate and appropriate for *all* types of technologies and business models for providers in scope, though other members confirm their support of TBEST and its continuation. Ofcom has also not indicated how frequently it expects providers to undertake TBEST going forward. We would consider a 2-3 yearly cycle with broader scope and more focused internal penetration testing to be reasonable and proportionate for a broad scope of services across the telecoms sector.
Consultation question 3: Do you have any comments on our proposed approach to enforcement?	*Is this response confidential? N* Everyone should share the goal of improving the security of UK networks through implementation of changes to the Communications Act (2003) in a timely manner. We need to foster a trusted and open culture across the industry where the identification of issues is seen as an opportunity for learning, rather than a threat to reputation and profitability, which tends to lead to attempts to restrict the provision of information. Ofcom's enforcement action should be evidence-based, proportionate, consistent, accountable, transparent and targeted. However, given the huge amount of sensitive information that providers will be sharing with Ofcom about their systems and processes, it would be unfair and inappropriate if Ofcom was to use this information to take formal enforcement action without first giving providers the opportunity to address any compliance concerns. Punitive enforcement action should be an absolute last resort, in cases where providers is both in breach of the Regulations and wilfully fails to take action towards compliance. In these circumstances we would support enforcement action on Ofcom's part. In general, the proposed approach to enforcement set out in the consultation provides every opportunity for regulated providers to mend their ways and work collaboratively with Ofcom. techUK recommends that Ofcom begins to engage with providers as soon as possible and

	to work in close collaboration with them, to minimise the risk of unnecessary and counterproductive formal enforcement action, for the benefit of both providers and Ofcom.
Consultation question 4: Do you have any comments on our proposed approach to reporting security compromises?	*Is this response confidential? N* techUK members feel that this proposed approach by Ofcom contains significant gaps and challenges for providers. It appears that Ofcom has focused on a set of thresholds that are identical to the existing outage reporting regime that providers are familiar with for many years, without adapting or updating this regime for cyber security incidents. For example, duration of incident may make sense when talking about the availability of a service, but may not be relevant when talking about a cyber incident that affects the confidentiality or integrity of a service. That said, quantitative criteria such as affected customers could be relevant and will certainly help providers concentrate on significant incidents, and prevent Ofcom from being overwhelmed with over-reporting. Members question the 'Qualitative criteria' in Annex 1 of Annex A5, specifically paragraph A1.1, and the inclusion of "security compromises attracting national mainstream media coverage' as a reason for notifying Ofcom of an "urgent" security compromise. Members point to recent "media-worthy" security compromises, such as SolarWinds and Log4j, which would not meet the thresholds laid out in Table 1. This suggests a disjoin between what Ofcom appears to want (visibility of significant security instance within providers) versus what has affected consumers. Further exploration is recommended on this proposed approach, including whether criteria based on potential media coverage is appropriate. Indeed, such qualitative criteria are harder to build into any automated reporting system (which ultimately is needed to meet the reporting thresholds and timescales). A general overarching concern facing many of our members is the increased duplication of requirements, compliance, and reporting with resulting from new security duties as enacted

by the Telecommunications (Security) Act 2021, and the proposal for legislation to improve the UK's cyber resilience.[5] The former will be monitored and enforced by Ofcom, while the latter is proposed to be enforced by the Information Commissioner's Office (ICO). Some organisations are already regulated by both organisations as Digital Service Providers (DSPs) and either as Public Electronic Communications Services (PECs) or Public Electronic Communications Networks (PECNs). They are already required to report cyber incidents under the Communications Act (2003), and under the Network Sharing and Information Systems Regulations (NIS).

There is already substantial scope for double reporting, as companies who find themselves regulated in this way must also report the same incident to the ICO. The government now proposes to add Managed Service Providers (MSPs) to the scope of the NIS regulations. As matters stand, the government risks creating a very substantial additional regulatory burden for PECS that happen to be MSPs as well. There are also ongoing discussions involving HM Treasury, the Bank of England and the Financial Services Authority around the imposition of similar requirements on Digital Service Providers serving banks and other financial institutions. This kind of double reporting of the same cybersecurity incident to multiple regulators with different sectoral responsibilities does nothing to support the Government's cybersecurity objectives. But it does create very substantial additional regulatory burdens.

The extent of this issue threatens to worsen. As Ofcom notes, The Telecommunications (Security) Act (2021 has strengthened reporting requirements on PECS and PECN providers which it reflects in Annex 5 to this consultation. In parallel, the government proposes to (in effect) widen the nature of incidents that would need to be reported effectively to both regulators by requiring digital service providers to report:

[5] https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/proposal-for-legislation-to-improve-the-uks-cyber-resilience

	“Any incident which has a significant impact on the availability, integrity, or confidentiality of networks and information systems, and that could cause, or threaten to cause, substantial disruption to the service.” techUK believes that Ofcom should, as part of its implementation of the Telecommunications (Security) Act, actively work with other regulators to ensure that it is not duplicating regulatory requirements for companies that are within both their jurisdiction, and those of other regulators because of the nature of service they offer. Ofcom’s membership of the Digital Regulators Co-operation Forum (DRCF) is designed to address issues in relation to regulatory coherence. This is one such issue. techUK encourages Ofcom to take a leadership role in such forums to raise this issue have it dealt with On a fundamental level, it is important that companies regulated by multiple agencies for cybersecurity have clarity what UK regulatory agency is responsible for cybersecurity incident reporting and response in the UK and that responsibility is assigned to that agency to co-ordinate and disseminate any information that a regulator or government department may need as a result of an incident occurring. To an extent, it does not matter which agency or department this is. That is something to be resolved by those bodies. A useful example of this kind of approach in action is seen in the context of the NIS II Directive proposed by the EU, where it has been made clear that cybersecurity incident reporting for telecoms service providers is no longer within the wider telecoms regulatory regime embodied within the European Electronic Communications Code (EECC).
Consultation question 5: Do you have any comments on our proposed approach to information sharing?	*Is this response confidential? N* techUK members are somewhat more comfortable with the Ofcom proposed approach to information sharing in the spirit of industry-wide efforts to protect the nation. However, in this spirit, it must also be noted

	that our members are concerned about the effect on Ofcom, as a valuable target, with its increased holding of data on incident reports, security compromises, S135 notices etc, and that this information is moved into a secure enclave as soon as possible. As an alternative, it would be more appropriate for the information to be stored by each provider in systems which they control, with access being controlled by the provider to named individuals within DCMS, Ofcom and NCSC. This is the approach taken for providers to share mitigation plans with DCMS/Ofcom/NCSC on the current TBEST project. While industry has received assurance that Ofcom will strengthen its security processes to counter this threat, this remains a concern for the regulator, industry and national security.
Consultation question 6: Do you have any other comments on our draft statement of general policy set out at Annex A5 to this consultation?	*Is this response confidential? N* No answer submitted.

Questions concerning Ofcom's draft guidance on resilience requirements in sections 105A to D of the Communications Act 2003 (see Annex A6).

Question	Your response
Consultation question 7: Do you have any comments on our proposed approach to resilience set out in section 4 of the draft guidance at Annex A6 to this consultation?	*Is this response confidential? N* techUK members are generally supportive of Ofcom's proposed approach to resilience in section 4 of Annex A6, as it relates to a well-established and adhered-to framework of resilience measures, including ENISA, NICC and the EC-RRG.
Consultation question 8: Do you have any comments on our proposed resilience guidance set out in section 5 of the draft guidance at Annex A6 to this consultation?	*Is this response confidential? N* Whilst recognising that Ofcom cannot give up-front advice on every matter of resilience, there are topics that would benefit from Ofcom driving common industry positions. For example: • Resilience of interconnection – there is a need for an industry debate on resilience of networks in case of interconnect failure.

- Resilience of access networks – there is a need for consistency in agreeing standards about the degree of network diversity that is proportionate for a handover involving network access partners.
- Power resilience – there are ongoing conversations with Ofcom in this area, as customers are increasingly encouraged to rely on their mobile devices when there is a power outage. Greater power-resilience is not cost-free, so it will be necessary for Government, Ofcom and other sector regulators to continue the conversation about the cost of power resilience.

From a general perspective, the resilience of a network or a service will be considered during the design and when establishing the architecture by which services will be delivered. The architecture of a network will evolve and only periodically be subject to any fundamental change. The TSA and the draft Regulations and Code introduce the term ‘security compromise’ that relates to both cyber-incidents and resilience incidents. Where either of these have a significant impact on the services available to end users, there are reporting obligations which will provide Ofcom with information on the duration, services impacted, customers impacted, cause of the incident and actions taken. The actions that can be taken to prevent a recurrence of an incident are likely to be dependent on the type of root cause and it must be appreciated that a Provider cannot take action to prevent a storm, pandemic or similar resilience factors. Of course, all telecoms services are dependent upon power being available and provisions can be made to remain operational during an interruption of power supplies and such resilience decisions will be clear.

The Procedural Guidance indicates that Ofcom expects to be far more engaged in all aspects of resilience and that Providers can expect to be required to provide explanations and documentation of decisions that may have been undertaken several years ago when the current network was still being established.

	The availability of records of such decisions may be difficult to provide. However, the architecture as is can be described (which is the result of such decisions made historically). We urge Ofcom to recognise such limitations and confirm that the resilience guidelines will not have retrospective effect.
Consultation question 9: Do you have any other comments on our draft guidance set out at Annex A6 to this consultation?	*Is this response confidential? N* techUK members are anticipating that the forthcoming National Resilience Strategy will also cover some of the areas covered by Ofcom's guidance. In particular, we note that the telecoms industry and its customers are heavily reliant on the electricity industry. We urge Ofcom to engage in the upcoming discussions in this domain.