BT Group Response

- Consultation on Ofcom's draft general statement of policy under section 105Y of the Communications Act 2003 (Ofcom's "procedural guidance"), and;
- Consultation on Ofcom's draft guidance on resilience requirements in sections 105A to D of the Communications Act 2003 (Ofcom's "resilience guidance")

Comments should be addressed to:
BT Group Regulatory Affairs
1 Braham Street
London, E1 8EP
Regulatory.affairs@bt.com

Introduction

- The establishment of a new baseline for telecoms security across the industry is necessary and BT fully supports the creation of the Regulations, the Code of Practice ('the Code') and the associated Ofcom Guidelines ('the Guidelines').

- BT continues to be at the forefront of sector-level security improvements and initiatives and, for many of the requirements set out in the draft Code, BT already complies or is on a path to compliance.

- Nonetheless, the requirements of the new Code are substantive and will require material investment by BT over a period of years. We therefore welcome Ofcom's proposed pragmatic approach towards applying its new duties in respect of the Guidelines during the early years of the regime.

- While we generally agree with proposals, we are concerned about the viability and suitability of the proposed **cyber incident notification regime**, both where operators are required to report incidents to Ofcom and where they are required to notify users of a 'significant risk of compromise'. These notifications risk unintentionally creating new security and resilience challenges as operators seek to comply with the regime.

- More broadly, there are several areas where **expectations of industry are unclear**. We would welcome clarity from Ofcom on these points in the final Guidelines.

Key points

1. Ofcom's proposed criteria for reporting cyber incidents will not achieve its desired objective

Where incidents will go unreported

1.1 The requirement for operators to use the number of affected users as a metric in assessing whether cyber security incidents are 'reportable' will result in most substantive incidents going unreported. BT's evidence suggests most such incidents do not result in any loss of service; rather, they impact the integrity of the network, result in a data breach, or cause no change in function whatsoever. The proposed accompanying qualitative criteria do not fully compensate for this lacuna.

1.2 [Redacted]

1.3 To better capture 'real world' security events, Ofcom should consider a framework reflecting criteria currently used by operators to identify high priority incidents as part of their own internal assessments. These include those focused on an operator's ability to trade or coordinate attacks targeted at a particular organisation/network element. []

Where incidents will be reported that should only be shared with national security agencies

1.4 Separately, there are some highly specific circumstances in which use of the formal security notification process outlined by Ofcom will not be appropriate, for example, where an incident leads to (or is likely to lead to) formal classification by a UK security agency. In these specific circumstances, providers should have discretion to liaise with

Ofcom outside the normal notification process. Given the severity of such incidents, this should take place by exception and via direct communication between providers and the relevant Director at Ofcom, and only at an appropriate time after the event.

2. Notifying users of all significant risks of a security compromise creates new harms

2.1 As currently envisaged, the new regime requiring alerts to be sent to users is likely to lead to the following outcomes in many cases;

- Alerts inadvertently revealing service/network vulnerabilities to malicious actors;
- Malicious actors imitating alerts to defraud users using channels used by operators for genuine alerts;
- Users becoming desensitised to major alerts which require action having received a high volume of alerts over the preceding period;
- Users taking inappropriate steps leaving them worse off where they receive an alert and misunderstand the best course of action.

2.2 Given the above risks, alerts are only appropriate where there is an explicit and clearly identifiable opportunity for users to take remedial action to mitigate the risk of compromise. Based on the Explanatory Note accompanying the Telecommunications Security Act ('the Act'), we understand that the primary intention of the user reporting process under s105J is to give users the opportunity to take remedial action. Otherwise, the cost to end users resulting from an alert might undermine any benefit gained from receiving it.

2.3 Furthermore, the lack of clarity in the Act is likely to lead to a wide range of discrepancies in how different providers inform users of such incidents which ultimately might undermine the entire process.

2.4 In its Final Guidelines, therefore, Ofcom should:

- make clear that there exists sufficient operator discretion in the Act to decide whether it is appropriate to send a given alert based on objective criteria relating to the costs/benefits to end users;
- use its convening powers to promote a common reporting standard for user reporting across industry to ensure that ambiguities in the current drafting is properly clarified, given the need for cross-industry alignment.

3 Ofcom's expectations of industry are unclear in five areas

Commencement date of new regime for reporting (Annex 5, Section 5)

3.1 The draft Guidelines[1] do not specify a date by which operators should have in place a system for reporting cyber incidents to Ofcom/significant risks of security compromises to users under s105J.

3.2 New notification regimes will take months for BT to integrate into our systems, given the need to train staff, introduce appropriate governance protocols, and establish reporting frameworks. Ofcom should provide clarity on the deadline for providers to introduce these measures in its Final Statement, setting this deadline at a reasonable period (i.e., at least 12 months) after commencement of the new regime.

Commencement date of compliance for Tier 2 providers (Annex 5, Section 3).

3.3 In its response to the Code consultation, BT advocated for Tier 1 and Tier 2 timelines to be aligned to reflect the significant change required and avoid the unintended effect of smaller providers, supplying or wholesaling to large operators, being de facto required to meet Tier 1 deadlines. Subject to the final Code and Regulations, Ofcom should update its Guidelines to reflect this change.

Treatment of jointly controlled third-party suppliers

3.4 As currently drafted, the Code *could* be interpreted to imply that MBNL – which is entirely controlled by BT and Three – should be treated as an independent third-party supplier rather than an extension of respective parent companies. BT's response to the Code makes clear that we do not intend to treat MBNL as an independent third-party given the strong degree of operational control exerted over MBNL. We urge Ofcom to consider the range of third-party supplier models currently in place of the market in carrying out its new security duties.

Use of the TBEST regime (Annex 5, Section 4)

3.5 To provide clarity for providers, Ofcom should detail specific criteria it intends to use in assessing whether schemes are equivalent to TBEST. This measure would also support market participants in understanding security measures in place in third-party networks.

Scope of the provisions/treatment of legacy and new model services (Annex 5, Section 3)

3.6 Given the need to ensure end-to-end security of UK networks, Ofcom should provide further clarity on how it interprets the scope of the Act to ensure a common understanding of where obligations apply is shared by market participants. It is not clear, for example, whether/how Ofcom intends to monitor providers offering novel services on a standalone basis[2], and what criteria will be used to assess whether provisions apply. Clarity on this point is needed given such services usually interconnect with the networks of 'full-service' providers.

3.7 More broadly, further detail is needed on:

- how Ofcom defines legacy services/how providers of them can demonstrate compliance given the flexibility provided by the Code;

[1] We note the FAQs on the website suggest the requirement might be in place by October 2021
[2] For example, providers offering eSIMs or 'over-the-top' services which interconnect with the PSTN

- how providers with a global footprint should demonstrate compliance alignment with international security standards, and;

3.8 Finally, it is not clear what provision Ofcom will make to provide transparency to industry on its evaluations and developing policy thinking once the final Guidelines have been adopted. As far as possible, Ofcom should continue to provide written feedback via to market participants to facilitate development common understanding of the requirements and drive good behaviours within the industry.

Consultation question 1: Do you have any comments on our proposed approach to compliance monitoring?	See paragraph 3.3-3.4, 3.6
Consultation question 2: Do you have any comments on our proposed approach to testing?	See paragraph 3.5
Consultation question 3: Do you have any comments on our proposed approach to enforcement?	None
Consultation question 4: Do you have any comments on our proposed approach to reporting security compromises?	See paragraphs 1.1-2.3 and 3.1-3.2
Consultation question 5: Do you have any comments on our proposed approach to information sharing?	None
Consultation question 6: Do you have any other comments on our draft statement of general policy set out at Annex A5 to this consultation?	None

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?	None
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?	None
Consultation question 9: Do you have any other comments on our draft guidance set out at Annex A6 to this consultation?	None

Please complete this form in full and return to securityconsultation@ofcom.org.uk