openreach
Connecting you to your network

Openreach's response to Ofcom's Consultation:

"General policy on ensuring compliance with security duties"

NON-CONFIDENTIAL VERSION

30 May 2022

Foreword

This response is provided by Openreach Limited - a wholly owned subsidiary of BT Group. We are a wholesale network provider and the vast majority of our products and services are regulated via price controls and/or regulated terms and conditions. We support more than 660 Communications Providers (CPs) helping them to connect their customers throughout the country.

We believe that everyone in the country deserves access to decent and reliable broadband – and our engineers work in every community, every day, to deliver our big bold plan for better service, broader coverage and faster speeds across our network.

Our people build, maintain and manage more than 197 million kilometres of fibre and copper wires. Over 14,600 service delivery engineers carried out 9.8 million engineering jobs last year through all seasons and in all weathers. Over the last decade our capital expenditure has been more than £15 billion as we focus on building and maintaining our networks.

1. Introductory Comments on Ofcom's proposals

Overview

1. Ofcom published its consultation document entitled *"General policy on ensuring compliance with security duties*" ("the Ofcom Consultation") on 8 March 2022. We welcome the opportunity to comment on the consultation which covers Ofcom's proposed policy and guidance ("the Guidelines") on the exercise of its functions under sections 105I and 105M to 105V of the 2003 Communications Act ("the Act") and the update to resilience requirements in sections 105A to 105D of the Act.[1]

2. Ofcom's Consultation is closely related to, and in part dependent on, a parallel DCMS consultation *"Telecoms security: proposal for new regulations and code of practice"* ("the DCMS Consultation") which deals with DCMS proposals for new security regulations ("the Regulations") and a new code of practice ("the Code").

3. We have already made a submission to DCMS on its consultation (submitted 10 May 2022) which included our views on specific technical, legal and regulatory points.[2] Therefore we do not repeat these arguments in detail in this submission. However, there are some important dependencies[3].

4. In particular we have a significant concern about the implementation timescales proposed in the DCMS Consultation for different Tiers of provider.[4] Our view is that DCMS should reconsider its proposed implementation timetable – and should the DCMS Consultation result in changes to its proposals, then we would expect Ofcom will also need to review and reset its proposed compliance timescales in line with the final DCMS outcome.

5. Also, whilst we broadly agree with Ofcom's proposals as set out in the Ofcom Consultation, we are concerned about the viability and suitability of the proposed cyber incident notification regime, both where providers 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 providers seek to comply with the regime.

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

7. Even so, it is timely and helpful that Ofcom has set out its proposals at this stage, so that providers can consider how best to meet the compliance, monitoring and reporting obligations required under the new security and resilience framework.

8. Openreach is already one of the most highly regulated businesses in the UK and hence the additional collective impact of these new interventions is significant for our business. Therefore, it is important that Ofcom and Government remain aware of these wider obligations and consider future interventions 'in the round' to ensure that any new burdens imposed are understood in that wider context, and are necessary and proportionate.

9. Nevertheless, we fully agree with the overarching objective of the new telecommunications security framework to create a new baseline for security and resilience of the UK's digital networks. Network security and resilience is a critical priority for both Openreach and the UK, and has always been placed at the heart of our operations.

---

[1] The new powers arise out of the introduction of the Telecommunications (Security) Act 2021 ("the TSA").
[2] BT Group has also made a separate submission.
[3] We would also be pleased to discuss our DCMS submission further with Ofcom and/or supply a copy of our non-confidential response.
[4] Please see the section headed 'Proposed Implementation Timetable in the DCMS Consultation' below where we explain our view in more detail.

10. The proposed new framework will, at an aggregate level, help to build on this strong foundation to make the UK's digital infrastructure even more secure – and we will continue to work closely with stakeholders, partners and other BT Group businesses to maintain the highest levels of security and resilience in our network.

11. Given the scale and scope of the Code, we also welcome Ofcom's proposed pragmatic approach to applying its new duties in the Guidelines.

12. For the most part, we believe we are already compliant with the proposed new Regulations, or have a clear path towards becoming compliant. However, we have identified some areas where further clarifications are required or where proposed regulations may be disproportionate or not achieve their intended effect. These points are discussed in more detail in response to the relevant questions in Section 2 below.

Proposed Implementation Timetable in the DCMS Consultation

13. We have an overriding concern with the timescales set out for compliance with the DCMS Code. While our network security and resilience are already high, there are some areas where we will need to carry out significant activity in order to be compliant and the current proposals do not permit sufficient time to do so. Currently, the proposed framework remains a draft set of requirements and consequently there is very little time to comply with those requirements due to be implemented by 31 March 2023.

14. This is especially true in cases where we need further clarification from DCMS before being able to assess what our obligations are (and the impact of consequential and dependent Ofcom policies).

15. Short implementation timeframes will add extra and unnecessary cost and risk to our development work, which could be mitigated through extensions to the current proposed deadlines. Meeting these new requirements under tight timescales will be placed under additional challenge as we continue to scale our build in support of the Government's broader digital commitments.

16. We also understand from wider engagement with the sector that many Tier 2 and Tier 3 providers are concerned that they will ultimately have to comply on the same timeframes as Tier 1 providers. While we cannot comment on the appropriateness of how our customers or competitors intend to comply with these requirements, we do think that aligning the timescales for Tier 1 compliance with the later dates proposed for smaller scale providers would have two positive effects by:

    - Enabling Tier 1 operators to have more time to respond and build on a strong foundation to make sure they can comply in as cost effective and proportionate manner as possible, and
    - Permitting Tier 2 (and if need be Tier 3) providers more time to comply if they assess that they need to align with Tier 1 timelines in order to continue using Tier 1 networks and services.

17. Consequently, should the DCMS Consultation result in changes to its proposals, then we would expect that Ofcom will also need to review and reset its proposed compliance timescales in line with the final DCMS outcome.

18. Overall, we see Ofcom's Consultation as the start of an important process rather than the conclusion and that there is more work to do involving Ofcom and industry. We are pleased that this is acknowledged by Ofcom, and we will be happy to play a proactive and constructive role in implementing the new framework.

2. Responses to Ofcom's Questions

Annex 5 – Procedural Guidance

Q1: Do you have any comments on our proposed approach to compliance monitoring?

Introduction

19. We note Ofcom's new duties under the Act and look forward to working with Ofcom to implement a pragmatic and workable framework for compliance monitoring. We also welcome Ofcom's acknowledgment that its approach needs to be based on working collaboratively with providers and gaining industry support to develop its processes rather than mandating a predetermined solution.

20. Time will be required on all sides to set up internal governance frameworks and processes to ensure compliance, and as Ofcom note in paragraph 3.6 the threats faced by operators will continually evolve - hence the compliance monitoring framework also needs to be able to evolve and where possible pre-empt threats rather than simply react to them.

Compliance Monitoring

21. We note that Ofcom makes various points in section 3 of Annex 5 about 'Tiering' and how it will guide Ofcom's approach to compliance monitoring. As referenced in our introductory comments above, we have significant concerns about the various compliance timescales proposed by DCMS for the different Tiers, and hence should DCMS change its proposals, then we would expect that Ofcom will also need to reconsider its proposed compliance monitoring timetable.

22. Nevertheless, there may still be opportunities for Ofcom and providers to carry out preparatory work for compliance monitoring in advance of any revised DCMS implementation and we would be very pleased to support any such initiatives.

Information Gathering

23. Openreach already receives multiple information requests across all its activities, and it is essential that this ongoing workload is recognised and planned for as part of this important exercise. We note that Ofcom's work in information gathering has been underpinned by the establishment of the Ofcom Information Registry Team (IRT) in 2020. Openreach values the work undertaken by the IRT and would like to build on this relationship when collating and exchanging information relating to the new security framework.

24. Therefore we support Ofcom's proposed approach to use its s135 information gathering powers to collate information and that it is important that Ofcom adopts what has become established as 'best practice' when issuing such requests. This means (i) where possible discussing the content and scale of proposed s135s informally with recipients before issuing a 'draft' request, then (ii) as part of the 'draft' s135 process ensuring that sufficient time is available for recipients to fully assess the viability of providing the information and of meeting the proposed timetable, and (iii) at the 'final' s135 stage allowing sufficient time for recipients to complete, validate and internally approve the completed response. Such a process seeks to enable respondents to supply complete, accurate and timely information.

25. As many of the requests may cover new ground, this information gathering framework may be more important than usual, and the preparatory steps will be essential to ensure that only necessary information is requested in the first place, and that the questions are fully understood and can be completed by the respondents. We expect that this will be of benefit to all stakeholders.

26. We also agree with Ofcom's proposal in paragraph 3.28 that 'follow up meetings' may help all parties understanding and interpretation of the information provided, and help refine and prepare for future information request cycles.

Commencement date of compliance for Tier 2 providers (e.g. including information gathering)[5]

27. In our response to the DCMS consultation, we are advocating for Tier 1 timescales to be aligned with Tier 2 (providing an additional two years for implementation) to reflect the significant changes required and to avoid the unintended effect of smaller providers, supplying or wholesaling to large providers, being de facto required to meet the much more challenging Tier 1 deadlines. The Tier 1 deadlines being unrealistic in our view and hence better for all to align to a more realistic and achievable timetable. Subject to the final outcome on the DCMS Code and Regulations, it would be important that Ofcom update its Guidelines to reflect any realignment or changes required.

Scope of the provisions and treatment of legacy and new services

28. The new regime diverges from the existing framework by placing the onus on providers to demonstrate compliance with the Code. Given this context, the interconnectedness of UK networks, and the need for end-to-end security, Ofcom should provide greater clarity on how it interprets the scope of the Act to ensure a common understanding of obligations is shared by market participants. In particular, further detail is needed on:

    - how Ofcom defines legacy services and how providers of them can demonstrate compliance given the flexibility provided by the Code;
    - how providers with a global footprint should demonstrate compliance alignment with international security standards; and
    - whether and when providers offering new novel service delivery models will fall within scope of the provisions.

29. 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 consider establishing a process for providing written feedback via the Ofcom website to market participants to facilitate the development of a common understanding of the requirements and drive good behaviours within the industry.

Treatment of jointly controlled third-party suppliers

30. In our response to the DCMS consultation we raise the point that the proposed Code as drafted might imply that a jointly owned company which is entirely controlled by higher Tier companies should be treated as an independent third-party supplier rather than an extension of respective parent companies. In our view this is not appropriate given the strong degree of operational control the parent companies would exert. An inappropriate classification would precipitate further vendor security assessments and present an unnecessary burden on both Ofcom and respective parent companies. Therefore, in its final Guidelines, our view is that Ofcom should clarify that jointly/wholly controlled third-party suppliers should be treated as an extension of the parent companies rather than as an independent third party.

Ofcom's Other Powers

31. We also note Ofcom's other powers as set out in section 3 of Annex 5 (e.g. powers of entry etc.) and consider that it is important to discuss these in more detail with Ofcom to better understand how and when it proposes to use such powers, in particular where these are new powers introduced in the Communications Act (and so, are not covered in Ofcom's current regulatory

[5] And also 'Enforcement' and other Ofcom implementation timescales.

guidance such as Ofcom's Enforcement Guidance for Regulatory Investigations). This would be beneficial to carry out before they are called into use to ensure all parties understand how Ofcom is intending to exercise its new powers and has had a chance to comment - in particular in relation to the rights and obligations of the providers investigated and of Ofcom itself. This should help prevent misunderstandings taking place in potentially serious and challenging situations at a later date when security compromises may have occurred or still be in progress.

Q2: Do you have any comments on our proposed approach to testing?

32. We note Ofcom's expanded powers under section 105N of the 2003 Act to monitor compliance and its proposal to continue with its voluntary penetration testing framework (known as 'TBEST').

33. We agree that suitable and proportionate 'penetration testing' and 'red teaming exercises' are key components in security assurance and the maintenance of a security framework. It should be expected by all parties that the Regulations need to be tested and audited appropriately by suitable internal and external bodies.

34. We also note and welcome that the draft Guidelines imply that providers might also use alternative approaches to TBEST as important security building blocks, which would be taken into account by Ofcom in its compliance assessments.

35. Therefore, given the wide range of approaches currently available, it would be helpful if Ofcom could provide clarity on what specific criteria schemes other than TBEST we would need to fulfil to be considered adequate and/or equivalent by Ofcom.

36. In summary, we do not foresee a major issue at this stage with Ofcom's developing proposals on testing as long as we, Ofcom and other providers can work together to find a pragmatic and proportionate framework. We would be pleased to discuss further with Ofcom as it's thinking develops.

Q3: Do you have any comments on our proposed approach to enforcement?

37. We note Ofcom's expanded powers extending to enforcement of sections 105A to 105D, 105J and 105K of the Act. We also understand that Ofcom may have to carry out enforcement actions at times in order to implement its new duties.

38. We take our security responsibilities seriously, and hence anticipate being able to support Ofcom in its duties through positive engagement with any reasonable and proportionate actions it needs to take. However there may be times, which we would hope would be rare in practice, when parties disagree about the facts of a specific situation and the preventative/corrective actions required. In any such situation(s), we agree that Ofcom's proposal for a three-stage process would be helpful - i.e. (i) notification of interim steps, (ii) allowing provider to make representations, and (iii) issuing a direction to take interim steps.

39. On a first pass, the proposed process seems to allow for appropriate engagement between the parties, but we note that Ofcom do not set out any proposed timescales at this stage. In due course, it would be prudent for Ofcom to do so, to help manage stakeholder expectations and future planning.

40. We note that the financial penalties permitted by sections 97, 105S and 105T(1) of the Act are very substantial[6] and we therefore urge Ofcom to consider its actions carefully should it be necessary to pursue this type of enforcement. It is certainly an important consideration, as with all financial penalties, whether funds might be better used by businesses to resolve operational challenges and/or mitigate customer harm, rather than exerting an extra financial burden on the industry.

Q4: Do you have any comments on our proposed approach to reporting security compromises?

Overview

41. We note the implications of sections 105J and 105K which place duties on providers to inform users about the risk of a security compromise and also to inform Ofcom of security compromises.

42. We agree that an appropriate notification framework is required, but this is a very complex and sensitive area to get right, and one where the 'devil is in the detail'. In our view Ofcom's proposals as set out in Annex 5, Section 5 are a good starting point but unlikely to achieve the desired security objectives for notification of users and/or Ofcom as they stand, and do need further review and development. We would be pleased to support any such initiatives.

Commencement date of new regime for reporting

43. Openreach and BT Group already operate systems and processes that, at least in part, aim to carry out the types of notification envisaged by the Act, and our preliminary view is that it will be these existing mechanisms that will need to be enhanced and developed to take account of the new Regulations. Further, because Openreach security compromises would almost certainly also be BT Group incidents then we will need to agree and implement such developments internally and across the BT Group.

44. The draft Guidelines do not specify a date by which operators should have in place a system for reporting cyber incidents to Ofcom and/or significant risks of security compromises to users under s105J. We anticipate these new notification regimes will take some months to integrate into our systems, given the need to train staff, introduce appropriate governance protocols, and establish reporting frameworks. We urge Ofcom to take account of these challenges and to provide clarity on the deadline for providers to introduce these measures in its Final Statement. Setting this deadline at a reasonable period after commencement of the new regime.

45. Turning to the detail of the proposals set out by Ofcom in Annex 5 (Section 5, A1, A2, A3). Our view is that the proposed processes, guidance and template are a useful starting point but will require further detailed discussion between stakeholders and redrafting before they are likely to be operationally effective and fulfil the desired security objectives.

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

46. 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. Cyber-related incidents rarely result in any loss of service for end users; typically, they impact the integrity of the network, result in a data breach for end users, or result in no change whatsoever (for example, where incidents have been identified via penetration testing). The accompanying qualitative criteria regarding media reporting/incidents reportable to third-party public agencies do not fully compensate for this lacuna.

[6] For example, for contravention of a security duty a penalty of up to a maximum of 10% of a provider's 'relevant turnover' is permitted and £100,000 per day for a continuing contravention. Other significant penalties are permitted for other types of contravention.

47. Given the complexity and diversity of cyber-related incidents, there are no numerical criteria which would cover all appropriate incidents. Nonetheless, to better capture 'real world' security events, Ofcom should consider a framework reflecting the criteria currently used by operators to identify the highest priority incidents in their own internal assessments.

48. For example, BT Group uses the following criteria to define 'priority one' incidents in its internal process:[7]
    - [✂];
    - [✂];
    - [✂];
    - [✂];
    - [✂].

49. Separately, there are some circumstances in which reporting security incidents to Ofcom as well as other public authorities will detract from ensuring a coordinated response due to the need for 'live' information-sharing between providers and public agencies. For example, where the National Cyber Security Centre (NCSC) is performing functions in relation to a national security incident, it should have discretion to determine what information can and should be shared with third-party agencies (including Ofcom).

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

50. As currently envisaged, the new regime requiring alerts to be sent to users is likely to lead to the following outcomes in some or all 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.

51. 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. Otherwise, the cost to end users resulting from an alert might undermine any benefit gained from receiving it. Based on the Explanatory Note accompanying the TSA, we understand that providing end users with an opportunity to take remedial action to be the primary intention of the user reporting process under s105J.

52. Therefore Ofcom should make clear in its Final Guidelines 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.

[7] [✂].

Q5: Do you have any comments on our proposed approach to information sharing?

53. We note Ofcom's duties and information sharing powers and support the restrictions which aim to limit both the circumstances which permit information sharing and the relevant bodies with which information can be shared.

54. As Ofcom discusses in section 7, some bodies are relatively non-controversial such as DCMS and NCSC. However as Ofcom sets out in s7.6 and 7.7 there may be situations which require further consideration. In this respect, we support Ofcom's proposed policy of notifying providers at the point of requesting the information. This seems an appropriate first step. In due course, we would be pleased to discuss and explore the potential types of scenarios that might occur with Ofcom, so that both parties may be able to pre-empt concerns in a timely way and at an early stage, rather than being under pressure to consider them in a crisis situation.

55. For example, we have already set up and are operating a flexible and pre-agreed approval process for sharing 'Connected Nations' information which is up and running and operating very quickly and efficiently. Although the security Regulations are potentially more significant and serious we think it could still pay dividends to explore such options and associated challenges early in the process.

Q6: Do you have any other comments on our draft statement of general policy set out at Annex A5 to this consultation?

56. Please see our responses to questions 1 to 5 above. We do not have any further comments to make at this stage.

Annex 6 - Resilience Guidance

Q7: 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?

57. We note Ofcom's outline approach as set out in Chapter 4. In particular:

- The use of Ofcom's section 135 powers seems appropriate to gather relevant information.
- We look forward to responding to Ofcom's proposed consultation on its 'Enforcement guidelines for regulatory interventions' in mid-2022, and helping to develop a workable and appropriate framework for Ofcom and all providers.
- We recognise and understand Ofcom's approach in focussing its revised guidance on Resilience Incidents, linking it to General Condition A3, and the potential benefits of utilising the guidance and best practice information provided by recognised industry bodies such as those listed in sections 4.13 to 4.16 (i.e. ENISA, EC-RRG and NICC).
- We note Ofcom's guidance that Regulations 3, 6, 7, 9 to 15 are also relevant to resilience policy and guidance.

Q8: 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?

58. We note the important points Ofcom makes in Section 5 concerning the responsibilities placed on providers by sections 105A to 105D of the Act, and the accompanying Regulations (in particular Regulations 3, 6, 7, 9 to 11, 13 to 15).

59. We agree with Ofcom (as discussed in section 5) that network resilience is both a broad and deep subject and is therefore a very important area for all providers to address. In this respect Openreach already has extensive internal and Group wide governance in place and does not underestimate the need to remain flexible and alert to new and existing resilience risks such as those mentioned by Ofcom in paragraph 5.37.

60. Hence we will continue to work proactively with internal and external stakeholders to explore such risks and where viable to review and implement appropriate controls to (i) reduce the likelihood and frequency of Resilience Incidents occurring and (ii) mitigate any consequential impacts should they occur.

61. Further we note the specific guidance Ofcom sets out in paragraphs 5.14 to 5.19 regarding 'supply chain and outsourcing' which is part of an important area of Government intervention at this time.

Q9: Do you have any other comments on our draft guidance set out at Annex A6 to this consultation?

62. Please see our responses to questions 7 and 8 above, and also question 4 where we make more detailed comments on incident reporting. In conclusion:

- We recognise the new and important responsibilities that Ofcom now have to fulfil, and we look forward to working with Ofcom to create a common and workable framework throughout the UK communications industry.
- We fully support the Government's ambition to enhance security and resilience in all communications networks in the UK and acknowledge that Openreach has a key role to play in implementing the Regulations in the UK. We will continue to proactively engage with stakeholders and relevant bodies to implement the new framework.
- Ultimately, despite Openreach's own proactive plans, we have a clear dependency on other providers, suppliers, manufacturers, and retailers to be in a position to fully implement the new Regulations and Code in the target timescales set out by DCMS and Ofcom in their respective Consultations.