Openreach's response to Ofcom's Consultation:

"Resilience guidance consultation and Call for Input on mobile RAN power back up"

Non-Confidential

1 March 2024

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 nearly 700 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.

We employ more than 37,000 people who install, support and maintain the wiring, fibres and connections which link tens of millions of homes and businesses in the UK to our customers' networks.

Our network is the largest in the UK. And we're constantly developing, building and maintaining it to provide the UK with the service and speeds it needs. We want to make sure that everyone, everywhere in Britain, can be connected, and we do that by building the best possible network to serve them.

1. Introductory Comments on Ofcom's proposals

1. Ofcom published its consultation document entitled *"Resilience guidance consultation and Call for Input on mobile RAN power back up"* ("the Consultation") in addition to its proposed guidance *"Network and Service Draft Resilience Guidance for Communications Providers"* ("the Guidance") on 8 December 2024. The documents represent Ofcom's exercise of its functions under sections 105Y and 1(3) of the 2003 Communications Act ("the Act") and the update to resilience requirements specified in sections 105A to 105D of the Act.[1]

2. Ofcom's Consultation also covers a *"… Call for Input on mobile RAN power back up"* . Openreach does not operate a mobile RAN[2] hence this section of the Consultation is not directly relevant to us. However, from our perspective as a provider of fixed public electronic communications networks (PECNs) we welcome the opportunity to comment on the Guidance.

3. Overall, we support Ofcom's proposals, but we are concerned about the clarity and proportionality of some parts of the Guidance. We discuss these points in more detail in response to the relevant questions in Section 2 below.

4. Given the scale and scope of the Guidance we welcome Ofcom's proposed approach to its application. In particular, we welcome Ofcom's acknowledgement (in Section 4.7 of the Consultation) that "*The proposed guidance is not the only way for communications providers to comply with their resilience-related security duties… and is not binding"* and that *"A communications provider may choose to comply with their resilience-related security duties by adopting different technical solutions or approaches to those specified in the proposed guidance".*

5. We do however understand Ofcom's positioning that the proposed Guidance is intended to set out the general framework it would expect to refer to when investigating compliance with the Act, and therefore that communications providers (CPs) would need to be prepared to explain their reasoning if they were using a different approach.

6. These are important points of context, as it is highly likely that only the network operator would have a full understanding of the evolution and complexity of its platforms and processes and the reasoning behind its existing set of controls. In this respect, we are already aligned with the Guidance, as we have always placed network security and resilience at the heart of our planning and operations. And they remain critical priorities as we continue to work with stakeholders, suppliers, customers, and BT Group businesses to maintain and develop standards for the future. We are also making strong progress towards compliance with the TSA Security Code of Practice (CoP), also referenced in Ofcom's Consultation.

7. Overall, we see Ofcom's Consultation and Guidance as part of this wider process to enhance network resilience and security in the UK, and it is helpful that Ofcom has set out its proposals at this stage so that CPs can consider how best to meet its expectations. We recognise and understand how important this is for us, our customers, end-users and the UK, and we will be pleased to play a proactive and constructive part in supporting Ofcom in fulfilling its new and enhanced role.

[1] The new duties came through the amended Communications Act 2003, supplemented by the Electronic Communications (Security Measures) Regulations 2022.

[2] BT Group has made a separate submission which will address both Mobile RAN power back and its views on the proposed resilience Guidance. Its response will also cover higher-level Group wide network and IT functionality. Hence the Openreach response will only address guidance relevant to Openreach's access and backhaul networks.

2. Responses to Ofcom's Questions

Draft Resilience Guidance – Consultation Questions

Introduction

8. The primary fibre access networks (i.e. the public electronic communications networks (PECNs)) operated by Openreach and subject to the proposed guidance are based on VDSL (FTTC), Gfast (FTTC) and GPON (FTTP) deployments. FTTC cabinets and FTTP splitters are discussed below under the section headed 'Access', and FTTx Head-Ends are discussed under the 'Aggregation and Backhaul' heading.

9. Additionally, Openreach also operates nationally available wholesale Ethernet Access, Ethernet Backhaul and Optical Spectrum Access (OSA)[3] networks.[4] These have a range of resilience options available as part of the product specification and are engineered and priced accordingly. Hence, we do not comment in detail on these specialised products in this response, as our expectation is that downstream CPs, including Mobile Network Operators (MNOs), will architect their networks appropriately by selecting the components they require from us to support the resilience requirements of their end-customers.[5]

Q1: Do you consider the measures in the proposed guidance relating to the resilience of the physical infrastructure domains to be appropriate and proportionate?

10. We already adopt very high standards and best practice in planning and operating our network and therefore, we broadly support Ofcom's approach to physical infrastructure resilience as set out in Chapter 4 (4.21–4.58) of the Consultation and Chapter 4.1 and 4.2 of the Guidance. This enables us to:

    - Design our networks resiliently,
    - Implement rigorous physical security,
    - Protect against loss of energy supply,
    - Factor in environmental risks arising from geographical features, weather and climate change, and
    - Protect Critical National Telecommunications Infrastructure (CNTI).

11. However, some points of Guidance relating to fixed network infrastructure need further clarification. These are discussed below:

Access

12. Ofcom is correct to note (Consultation 4.23) that the scale and geographical reach of fixed access networks can make it disproportionately costly and complex to engineer fully resilient network architectures. Hence there will inevitably be single points of failure.

13. These risks can be mitigated against by a balanced network design which minimises numbers of customers impacted by a single point of failure, and consistent monitoring of the performance of

[3] Typically, these are based on Wave Division Multiplexing (WDM) technologies.
[4] These are also considered to be PECNs.
[5] For EAD, EBD and OSA - Openreach provides various resilience options to industry. These provide fibre and equipment resilience protecting against potential failure. Multiple duct routes are used if they are available, otherwise there will be passive commonality in the duct route until any divergence points are available in the network.

the networks, backed up by a range of repair and restoration processes which can be activated very quickly to restore service.

14. This approach means that for live broadband fixed access networks in the UK there is no significant deployment of 'automatic failover' at the FTTC cabinet or FTTP splitter level. It is not supported today and would be hugely cost prohibitive to achieve. We do operate some path level protection on backhaul for cabinets and Subtended Head-Ends (SHEs) where a Link Aggregation Group (LAG) exists across the fibre cables (i.e. protecting against single fibre loss) but our position is this is an optional feature and not a standard architecture given the restricted numbers of customers potentially impacted. Therefore, in our view, the proposals set out in the Consultation (4.26) are not proportionate or feasible for this element of the access domain given the limited number of customers impacted and the high level of additional investment required. To explain further:
    - For FTTC - all Openreach cabinets are currently parented off single Head-Ends as the per cabinet end-customer coverage and count is significantly restricted by geography and volume. We do not propose to implement dual parenting on these cabinets for these reasons and because of the significant level of cost required.
    - For FTTP – there are very low numbers (a few tens) of end-customers on a single Openreach PON structure, and additional redundancy at the splitter level would in all likelihood use fibres existing on the same cables and using the same ducts as a single splitter, providing little or no resilience benefit. Therefore, as above we do not propose implementing redundancy at this level in the network for these reasons and because of the significant level of cost required.
    - The appropriate level of resilience/redundancy for FTTP Subtended Head-Ends (SHEs) also requires careful consideration. As above, fibres routed away from the SHE towards the exchange will in all probability be part of the same cable and same ducts providing little or no additional resilience. Given this, and the fact that the number of customers on any one structure is typically less than five hundred, means that it would be ineffectual and disproportionate to try and engineer such redundancy into the deployment.
    - Also, it is important to note that managing the handover of traffic to CPs in a dual parented model at this lower level in the access network is both technically very complex and introduces significant cost by the doubling up of Head-End ports for both Openreach and our CP customers. It also introduces the additional non-trivial challenge for a CP of predicting and managing where traffic might appear at any moment in time (e.g. Ipswich or Colchester, Manchester or Liverpool etc.).
15. For these reasons, we think it is important that the Guidance adds further clarification to better reflect the real state of play for fixed access networks in the UK. Although the Guidance discusses the trade-offs which need to be made between levels of redundancy and customer numbers, the text tends to imply that the base level assumption is that CPs are expected to architect FTTC based networks to meet a much higher default level of resilience than is currently viable (or likely to be viable) for national scale access networks (Guidance 4.2.1).
16. With regard to Ofcom's power backup Guidance for cabinets (4.2.1) we proactively deploy built-in battery power backup to cabinets, and also task our engineering teams with actively intervening in the network should the power supply fail for longer than the battery backup can sustain.
17. These additional support processes are important as a 4 hour battery specification does not necessarily mean that in a live situation, all batteries will perform at that level. This is because each

cabinet and power loss scenario will be unique.[6] Actual performance will be influenced by the age of the battery, the state of battery charge when the power failure occurs, and the real-time load on the battery during the power failure. Hence alternative power backup processes are also likely to be required in certain scenarios in order to maintain service for a full 4 hours following a power failure.[7]

18. In this respect, we note that Ofcom's text in the Consultation and Guidance variously refers to both 'battery' backup (e.g. Consultation 4.56) and 'power' backup (e.g. Consultation 4.57), with a strong inference that 'battery' backup is the preferred, and perhaps only solution. In our view it would be better for the Guidance to more clearly allow for alternative processes and solutions to support 4 hour 'power loss' resilience - thus enabling CPs to deploy batteries and/or other hybrid solutions that are appropriate for their network design (i.e. recognising the operational scale and complexity discussed above).

19. We note and agree with Ofcom's view in the Consultation (4.57) that many active cabinets (both for Openreach and other CPs) are increasingly likely to become secondary sources of broadband and telephony connectivity as Openreach's (and other CPs) full fibre rollouts continue to reach 25 million premises by 2026, and ever greater numbers by 2030. However, we would not expect a significant reduction in Openreach cabinet numbers during that period, as CP and end-customer migration is likely to continue to be challenging up to the end of the decade and beyond. Therefore, in our view it would be helpful if Ofcom's Guidance recognised the likelihood of this outcome for existing access networks and clarified that CPs are not expected to reengineer their access networks during major technology transitions to meet a higher default level of resilience, as this would result in major diversions of CP resources and potentially high levels of stranded costs.

<u>Aggregation and Backhaul</u>

20. We agree with Ofcom's view in its Guidance (4.2.2) that there should be a greater expectation of resilience higher up the aggregation chain, including measures to enhance resilience for equipment, connectivity and power loss.

21. This is in line with Openreach's approach. We already adopt very high standards and best practice in planning and operating the aggregation and backhaul elements of our networks, and in particular deploy significant levels of resilience at the head-end and exchange level.[8] These include inbuilt redundancy in head-end equipment and management resilience where appropriate, and substantial power backup strategies including battery banks, diesel generators and refuelling capabilities.

22. As noted above, we also provide a variety of Ethernet and Optical backhaul products for downstream CPs, including MNOs, to select the components they require from us to architect their networks to meet the resilience requirements of their end-customers.[9]

23. Additionally, another typical component for CP aggregation which is purchased from Openreach is Cablelink. This links the Openreach fibre head-end to an individual CP's network equipment. Openreach offers multiple Cablelink products if required, and therefore CPs are able to plan ahead to spread their traffic loading and therefore limit the impact of any individual port failure. This means the risk and potential impact is determined by CPs' network architecture in terms of their Cablelink configuration and customer loading.[10] We are considering the introduction of LAG

[6] For example, Openreach operates over 100k powered cabinets of different ages and in highly variable deployment environments and circumstances.
[7] Equally, in some scenarios where a DSLAM has lost mains power there is a possibility that the local customer base will also have lost power to their routers and other devices rendering cabinet power back-up ineffective.
[8] BT Group response will comment more fully on exchange level resilience in their response.
[9] See Footnote 5 above.
[10] Typically, this might be of the order of one to two thousand customers on a 10GE Cablelink.

functionality for Cablelink, but it is not currently available. Looking further ahead, the provision of cost-effective protection for Cablelink connectivity is likely to require industry level agreement to find a solution which will meet both Openreach and its CP customers' needs.

Q2: Do you consider the measures in the proposed guidance relating to the resilience at the Control Plane to be appropriate and proportionate?

24. We support Ofcom's approach to Control Plane resilience guidance as set out in Chapter 4 (4.59–4.83) of the Consultation and Chapter 4.3 of the Guidance and agree that a resilient Control Plane is important in maintaining the resilience and availability of CP networks.

25. Within Openreach, there is no interaction of the Control Plane with User Plane devices for routing of traffic (for FTTC and FTTP) with the exception of multicast. Therefore, static traffic paths are pre-configured for data transmission. Within the network elements the technology allows for redundancy of equipment controlling routing/traffic paths. This is used in the FTTx head-end to protect against single switch card failure, but not in active FTTC cabinets due to customer density and the lower-level risk and impact associated with a cabinet failure. It should also be noted that FTTC technology and the Openreach platform has now reached a point in its lifecycle where no significant developments are likely to be undertaken by vendors to introduce new functional software or hardware that might be required for resilience purposes at the cabinet level. For our Ethernet and Optical services there is no Control Plane function, as no control decisions are made based on user traffic, as all configurations are statically defined.

26. We note Ofcom's references to the TSA CoP in the Consultation and Guidance. We have a clear path towards achieving compliance with this important framework for security and resilience and agree this will also help support the general resilience of networks, including the Control Plane, along with the User and Management Planes.

27. We also refer Ofcom to BT Group's response for further comments on resilience Guidance applying to the Control Plane, as many of Ofcom's proposals refer to functionality which sits above the Openreach wholesale layer, such as signalling and messaging protocols, overload protections and systems interoperability amongst others.

Q3: Do you consider the measures in the proposed guidance relating to the resilience of the Management Plane to be appropriate and proportionate?

28. We broadly support Ofcom's approach to resilience guidance for the Management Plane as set out in Chapter 4 (4.84–4.104) of the Consultation and Chapter 4.4 of the Guidance and agree that a resilient Management Plane will help maintain the resilience and availability of CP networks in many circumstances. However, we think that the Consultation and Guidance does appear too prescriptive in parts.

29. In particular, we note that Ofcom explains in its Consultation (4.101) that it is not prescribing a particular type of 'out-of-band' (OOB) management system, and that it also recognises that manual approaches to restoring services may also be appropriate in certain circumstances. However, this acceptance of flexibility in approach seems to be overturned later in the same paragraph where the strong expectation seems to be that larger CPs should adopt OOB systems for the Management Plane. In our view the situation for live networks is more nuanced than that. For example, at the current time Openreach utilises both OOB approaches and other approaches to resilience:

- For our Ethernet and Optical services - we use an OOB ADSL management network today, and plans to migrate to SOGEA, SOTAP and FTTP are in the development pipeline.
- Whereas for FTTC and FTTP services:
    - We use in-band management of devices up to the fibre head-end because the provision of an OOB management network to over 100k cabinet sites would be prohibitively expensive and complex. We believe our in-band network to downstream devices has proven robust over many years and do not currently see a business case to manage these devices differently. We are also able to access a rich data set from other information feeds (e.g. from the head-end and downstream device telemetry) that would indicate any issues with the management network, and
    - For the fibre head-end there is an OOB management network connecting into a management infrastructure which consumes a core network capability from BT Group.
- With reference to Ofcom's comment in paragraph 4.104 of the Consultation, our view is that losing management connectivity will not immediately impact customer traffic or cause an outage. Although, we agree it would impact the ability to troubleshoot and provide new service.

30. We agree with Ofcom (Consultation 4.87) that CPs will need to consider utilising alternatives to PSTN lines (analogue and/or ISDN) in anticipation of PSTN switch-off, as they were often a straightforward and economic method for providing OOB management functionality.
31. We also note Ofcom's references to the TSA CoP in the Guidance (4.4) and agree this will help support the resilience of the Management Plane, along with the User and Control Planes, and wider network resilience.

Q4: Do you consider the measures in the proposed guidance relating to communications providers' own managed services to be appropriate and proportionate?

32. BT Group and other downstream CPs' responses will be more relevant to Q4 than Openreach's, but in so far as the Guidance applies to Openreach we support Ofcom's approach to resilience guidance for CPs' own managed services as set out in Chapter 4 (4.105–4.118) of the Consultation and Chapter 4.5 of the Guidance (subject to some clarifications set out below).
33. The primary focus of this part of the Guidance from an Openreach perspective is on the PECNs that Openreach operates in support of downstream VoBB services (and potentially other Specialised Services which Ofcom may consider to be covered by the Guidance).
34. Our FTTC and FTTP Generic Ethernet Access (GEA) service is only one part of the VoBB value chain, but it is an important element. Hence, we ensure that it is resilient and secure in line with the TSA CoP and Ofcom's Guidance by enabling CP controlled traffic prioritisation, service separation from the wider internet, resilient network management systems and processes, and robust service restoration processes and systems. In particular, and relevant to Ofcom's Guidance, is that the prioritisation markers supported by our GEA wholesale service enables CPs to differentiate and prioritise voice traffic over other traffic when using the GEA service.
35. As for our Ethernet and Optical services, from our perspective these are uncontended connections into CPs' access and/or core switches, and it is up to the individual CPs to decide the shaping and priority of traffic flows depending on the nature of the services they are providing.
36. With reference to some of the terminology used in the Consultation and Guidance, we initially found usage of the "CP-managed" services terminology to be unclear. For example, it included a

broad definition of services run by CPs independent of the internet as well as authentication/authorisation functions, and later references to "mobile services" and "critical services". It was also unclear to us to what degree "Specialised Services" were also impacted by the Guidance. However, Ofcom's clarification of its CP-managed services terminology and further explanation posted on the Ofcom website on 9 February 2024 was very helpful. We now understand that Section 4.5 of the Guidance considers that Specialised Services are intended to fall under the CP-managed services classification - but that not all Specialised Services will require a higher level of resilience. Rather it is up to CPs to assess which services are critical and therefore which require an enhanced level of resilience.

Q5: Do you consider the measures in the proposed guidance relating to communications providers' arrangements for preparing for adequate process, skills and training to be appropriate and proportionate?

37. Overall, we agree with Ofcom that CPs' processes, skills and training are important aspects of designing, implementing and operating resilient networks. Hence, we broadly support Ofcom's proposals as set out in Chapter 4 (4.119–4.148) of the Consultation and Chapter 5 of the Guidance. However, we do set out a few points of detail which are covered further below.

38. We have already implemented a wide range of controls and resilience measures that the Guidance proposes across our IT and network lifecycles to ensure that we can architect, design, test, deploy and operate high quality and robust services at the required service levels. We also plan and operate networks in ways that ensure services are robust under peak traffic loads and resilient to foreseeable extreme events.

39. Hence, we strongly support Ofcom's approach of avoiding prescribed standardised measures that apply uniformly across all use cases and CPs (Consultation 4.144) and that the proposed guidance around change management, training, asset identification/management, and life cycle management are all expected to be tailored by CPs to suit their particular circumstances.

40. This is very important as CPs need to be able to make informed judgements on which measures they need to introduce, or need to change, based on a detailed knowledge of their existing controls, which are informed by their own risk assessments. This is essential in enabling CPs to take balanced and proportionate decisions for their individual circumstances (by technology, architecture, customer density, cost etc). Ofcom's proposal of guidance measures based on widely recognised industry standards (such as ITIL) is a helpful steer, but as Ofcom notes (Consultation 4.148) experienced CPs (such as Openreach) will have been operating complex networks for many years and will already have many different measures in place to ensure resilience and service quality. This is where Ofcom's recognition that different approaches may be acceptable is helpful, allowing for a high degree of flexibility for individual circumstances.

41. Ofcom sets out a wide range of proposals in Section 5 of the Guidance, and we agree that they are all important to consider. However, we set out some points of clarification and detail below.

42. Capacity Management (Guidance 5.1.1.2) - we agree capacity management is essential, and hence it is already an integral part of Openreach's control mechanisms for all network components and functions.

    - However, it is not a reasonable expectation that CPs can plan and build excess capacity for any eventuality. This would be disproportionate. CPs can take all reasonable measures to anticipate increases in loading but will also need to use other measures to optimise existing capacity such as traffic management, application of different prioritisation markers and in exceptional

circumstances harsher traffic management/traffic blocking to preserve the integrity and security of the network (e.g. in the event of loss of a core site). Therefore, it would be helpful if the Guidance was clearer that building capacity is not the only solution when it comes to accommodating extreme events (e.g. such as "super-peaks")[11] as such investment is likely to be inefficient, and the capacity very likely to remain unused after the event. With the right end-customer incentives in place and reasonable traffic management by CPs, there are likely to be much more efficient measures that can be taken to reduce the overall network impact.

- From the Openreach perspective, we also look to CPs using our wholesale services to help manage capacity planning, by implementing reasonable procedures and practices to balance the loading of their Cablelinks and ports which connect into the Openreach network.

43. Supplier Management (Guidance 5.1.1.5) - we agree supplier management is important, but the range of tests and measures set out appears overly prescriptive given the wide variety of circumstances, network architectures, and other measures which can be adopted (e.g. pre-contract award testing, contract provisions, due diligence of suppliers' technical information etc). As Ofcom notes in the introduction to its guidance, ultimately CPs will need to make independent and risk-based decisions based on their detailed knowledge of their own networks and take appropriate measures. Hence the wording is this section could be more open, making it clear that CPs can ensure appropriate supplier management oversight and resilience through other measures.
44. Network Oversight Functions (NOFs) - we note that the Guidance (5.1.2, 5.2.2, and 5.3.2) makes reference to 'tools' that are likely to be considered NOFs for the purposes of the TSA CoP. We question whether the Guidance is the appropriate document for this conclusion. This could lead to confusion and an unintended consequence of expanding the range and definition of NOFs outside of the TSA process.

[11] For example, the coincidental timing of the launch of a new game and its download, and a high profile live streaming event.

3. Summary and Conclusion

45. We note Ofcom's approach[12] to its new duties under the Act as set out in its *"General statement of policy under section 105Y of the Communications Act 2003"* and *"Ofcom's Regulatory Enforcement Guidelines for Investigations"*. We recognise these new and important responsibilities that Ofcom now has to fulfil, and the extensive powers which it can use to carry out its duties[13], and we will look to support Ofcom in its duties with any reasonable and proportionate actions it needs to take.

46. More broadly, the resilience and security threats faced by operators will continually evolve and the industry needs to remain flexible and alert to newly emerging risks. Hence CPs need to have the flexibility to change and adapt according to their circumstances, and where possible pre-empt new threats. Therefore, it is an important element of the Consultation and Guidance that they recognise that CPs ultimately need to make informed judgements about resilience, taking account of best practice and guidance, based on the in-depth knowledge of their own infrastructure and risk assessments. Therefore, the points we raise in this response regarding levels of network redundancy and power backup are important points for Ofcom to consider to ensure the Guidance remains appropriate and proportionate.

47. In conclusion, we fully support Ofcom's ambition to enhance resilience and security in all UK communications networks and acknowledge that we have our part to play. We will continue to proactively engage with stakeholders and relevant bodies and look forward to working with Ofcom on these matters. We would be pleased to discuss any of the points made in this response with Ofcom in more detail if required.

[12] See Guidance Section 6.
[13] Including for example its information gathering powers, powers to enter premises and enforcement powers amongst others.