Virgin Media O2 response to Ofcom's consultation

General policy on ensuring compliance with security duties

Non-Confidential version

31st May 2022

EXECUTIVE SUMMARY

Virgin Media O2 ("VMO2") welcomes the opportunity to respond to Ofcom's consultation on general policy on ensuring compliance with security duties. Our networks and services provide vital connectivity for around 46 million customers (both consumers and businesses) and the importance of the services we provide is only going to increase in the coming years. We understand how vital it is that we keep our networks and the data they carry secure, and we support the Government's ambition to improve telecoms security in the UK – and indeed the security of UK plc as a whole.

Ofcom is consulting on new guidance for telecoms providers ("Providers") following the introduction of the Telecommunications (Security) Act 2021 (the "Act"). Specifically, Ofcom is consulting on the procedures it expects to follow in carrying out monitoring and enforcement activities, including guidance on which security compromises it would expect Providers to report. Ofcom is also proposing to update guidance on network resilience to reflect the new security framework.

We split our response to these documents, first, addressing Annex 5: Draft general statement of policy ("Procedural Guidance"), and second, addressing Annex 6: Draft Ofcom guidance on resilience requirements ("Resilience Guidance") (together the "Guidance").

We agree with the overall approach Ofcom has taken. We have a number of specific practical, technical and drafting comments on the two documents, which we set out in our response below, but in general, we welcome and support the approach Ofcom has taken.

Collaboration will be essential

We agree with Ofcom's proposed collaborative approach[1] and believe this will foster more compliant behaviours and reduce the need for regulatory interventions. However, we urge Ofcom to take this a step further and use a "collaboration-first" approach to its monitoring and enforcement duties under the Act generally, whether this relates to the Security Measures Regulation ("Regulation"), Code of Practice ("Code") or Guidance.

Information requests will require collaboration

We do not believe that an arms-length approach, based on statutory demands for information, is sufficient, or an effective means of monitoring compliance with the Act in the absence of collaboration. Detailed information requests can be extremely resource-intensive for both Ofcom and the Provider. We expect that the information requests relating to compliance monitoring will be very complex and even more resource-intensive, for Ofcom and for the Provider, given the breadth of information Ofcom is likely to need to assess compliance with the security framework. If the correct questions are not asked at the outset, with prior knowledge of a Provider's architecture, systems and processes, further questions must then be asked, increasing the workload for both Ofcom and the Provider. Equally, without context, the questions and answers may not be sufficient to enable Ofcom

[1] Introduction to the Consultation and paragraphs 3.5 and 3.7 of the Procedural Guidance

to adequately assess compliance. A collaborative approach throughout the process - and in particular before any information request is issued (in draft or otherwise) - will help to ensure that Ofcom obtains sufficient information about Providers' networks, services and systems to frame the questions from the outset, targeting the information most relevant to assess compliance in the format that the Provider is best able to provide it, which will reduce the need for time-and-people-intensive manual processes. This results in a more efficient process for both Ofcom and Providers, which is essential bearing in mind: (a) resource challenges (which we discuss further in our response below); and (b) that the people who will need to provide this information to Ofcom are likely to be the same people who are being tasked with implementing multiple new security requirements within very challenging timescales - and without impacting availability or customer experience.

Providers will need practical guidance

The supervisory model introduced by the Act is a step change for both providers and for Ofcom. We believe it is essential that providers can discuss with Ofcom how to interpret and implement the new requirements, and whether in some cases an alternative approach to the Code requirements might be appropriate and compliant. This will require an ongoing collaborative approach.

We therefore suggest that Ofcom expands its proposed collaborative approach to the telecoms security framework to create a mechanism by which Providers can discuss with Ofcom (on a bilateral and an industry-wide basis, as appropriate) any specific challenges with scope, definition and implementation and any general principles can be shared with industry as a whole to ensure consistency. This is the most efficient means of ensuring compliance. However, Ofcom's approach to compliance in recent years has been not to give specific guidance, and when approached by Providers, Ofcom's response has been to state that Providers need to take their own legal and regulatory advice. We urge Ofcom to embrace the different and more collaborative approach envisaged under the new security framework and supervisory model and create a mechanism under which Ofcom and Providers can work closely together, particularly in the first few years of implementation, to: (a) help answer the many new practical and technical questions raised by the security framework; (b) share that information to ensure a consistent interpretation of the requirements across the whole industry; and (c) ensure Ofcom has an in depth understanding of the complexity of Providers' architecture and systems and what it would involve to make changes (including the risk of potential impact to customers). We would welcome Ofcom's view on introducing such a mechanism, as a tangible method to foster collaboration. As currently drafted, no such mechanism is envisaged.

We support the ambition to improve security

We share Government's ambition to improve the security of UK telecoms networks and services and believe that with a limited number of changes, Government can ensure the Code and timing for implementation is proportionate, appropriate and practically achievable for all providers.

Timing of implementation is key to proportionality

We note that the proposed commencement date for the majority of provisions in the Act is expected to be 1st October 2022 ("Commencement Date") and Ofcom plans to issue final Procedural Guidance and Resilience Guidance in Autumn 2022. It is likely, therefore, that we will only receive the final Guidance on or around the Commencement Date. This raises practical challenges as Providers will need time to make process, procedural and system changes to comply with the new requirements. Ofcom acknowledges in the introduction to this consultation and in paragraph 3.7 of the Procedural Guidance that over the first few years of the regime Providers will "continue to work towards full compliance"[2] but it is not clear whether this statement only relates to Code requirements in Section 3 (which have stated implementation dates after the Commencement Date), or whether it should be interpreted more broadly.

Compliance with all the specific measures set out in the Regulation and Code is more complex for proposed Tier 1 Providers than smaller Providers. We welcome Ofcom's acknowledgment that due to the scale and complexity of many Provider's operations it is likely to take time to fully achieve improvement.[3] The size and scale of our networks, services and component systems, the legacy of multiple mergers and acquisitions and the need to review and adapt our many existing security controls, processes, and measures (including supply chain) to comply with the specific requirements of the new Regulation and Code mean that it is time, and not necessarily money, larger Providers need to ensure compliance in a way that does not adversely affect availability or customer experience for many millions of customers. Smaller Providers will not face this same complexity or the same scale of risk to customers.

The draft version of the Code was first seen by Providers on 1st March 2022. Until we receive the final Regulation, Code, Procedural Guidance and Resilience Guidance, we cannot be sure of the exact scope and detail of the requirements and therefore cannot finalise our impact assessments and implementation plans for the required procedural and system changes.

We urge Ofcom to acknowledge clearly in the Procedural Guidance and indeed in the Resilience Guidance (where there are changes to the 2017 Security Guidance) that there are multiple obligations within the new security framework (not only those set out in section 3 of the Code) where there is likely to be a journey towards compliance after the Commencement Date and full compliance will take time. We appreciate Ofcom's acknowledgement of this in paragraphs 3.5 and 3.7 of the Procedural Guidance, but we are concerned the wording used could be interpreted as only applying to Section 3 of the Code (which have stated implementation dates after the Commencement Date) and not to the requirements more broadly.

VMO2 recommendations

We support Ofcom's general approach to the Guidance and recommend that Ofcom should: (a) as discussed above, expand upon its stated commitment to a collaborative approach in more detail in the Guidance; and (b) amend paragraphs 3.5 and 3.7 to make clear that it will be a journey towards

[2] Introduction and paragraph 3.7 of the Procedural Guidance
[3] Paragraph 3.5 of the Procedural Guidance

compliance with the Act, Regulation, Code and Guidance after the Commencement Date and full compliance is not expected immediately.

Additionally, we would like to work with Ofcom as soon as possible after this consultation closes to ensure:

- we have interpreted the requirements correctly
- interpretation is consistent across industry; and
- discuss plans for implementation.

Given the extremely short timetable for implementation we would welcome both bilateral meetings with Ofcom and industry-wide forums for discussion, led by Ofcom (whilst at all times remaining fully compliant with competition laws).

VMO2

MAIN RESPONSE

INTRODUCTION

VMO2 welcomes the opportunity to respond to Ofcom's consultation on general policy on ensuring compliance with security duties. Our networks and services provide vital connectivity for around 46 million customers (both consumers and businesses) and the importance of the services we provide is only going to increase in the coming years. We understand how vital it is that we keep our networks and the data they carry secure, and we support the Government's ambition to improve telecoms security in the UK – and indeed the security of UK plc as a whole.

Ofcom is consulting on new guidance for telecoms providers following the introduction of the Act. Specifically, Ofcom is consulting on the procedures it expects to follow in carrying out monitoring and enforcement activities, including guidance on which security compromises it would expect providers to report. Ofcom is also proposing to update guidance on network resilience to reflect the new security framework.

We split our response to these documents, first, addressing the Procedural Guidance and second, the Resilience Guidance.

We agree with the overall approach Ofcom has taken. We have a number of specific practical, technical and drafting comments on the two documents, which we set out in our response below, but in general, we welcome and support the approach Ofcom has taken.

Collaboration will be essential

We agree with Ofcom's proposed collaborative approach[4] and believe this will foster more compliant behaviours and reduce the need for regulatory interventions. However, we urge Ofcom to take this a step further and use a "collaboration-first" approach to its monitoring and enforcement duties under the Act generally, whether this relates to the Regulation, Code or Guidance.

Information requests will require collaboration

We do not believe that an arms-length approach, based on statutory demands for information, is sufficient, or an effective means of monitoring compliance with the Act in the absence of collaboration. Detailed information requests can be extremely resource-intensive for both Ofcom and the Provider. We expect that the information requests relating to compliance monitoring will be very complex and even more resource-intensive, for Ofcom and for the Provider, given the breadth of information Ofcom is likely to need to assess compliance with the security framework. If the correct questions are not asked at the outset, with prior knowledge of a Provider's architecture, systems and processes, further questions must then be asked, increasing the workload for both Ofcom and the Provider. Equally, without context, the questions and answers may not be sufficient to enable Ofcom

[4] Introduction to the Consultation and paragraphs 3.5 and 3.7 of the Procedural Guidance

to adequately assess compliance. Information requests alone are not sufficient to enable Ofcom to understand the complexity of Providers' architecture and systems and what it would involve to make changes (including the risk of potential impact to customers).

Appropriate and proportionate enforcement will require a deep understanding of a Provider's network architecture and systems that cannot be obtained from information requests alone. A collaborative approach throughout the process - and in particular before any information request is issued (in draft or otherwise) - will help to ensure that Ofcom obtains sufficient information about Providers' networks, services and systems to frame the questions from the outset, targeting the information most relevant to assess compliance in the format that the Provider is best able to provide it, which will reduce the need for time-and-people-intensive manual processes. This results in a more efficient process for both Ofcom and Providers, which is essential bearing in mind: (a) current resource challenges (which we discuss further in our response below)[5]; and (b) that the people who will need to provide this information to Ofcom are likely to be the same people who are being tasked with implementing these multiple new security requirements within very challenging timescales – and without impacting availability or customer experience.

Providers will need practical guidance

The supervisory model introduced by the Act is a step change for both providers and for Ofcom. We believe it is essential that providers can discuss with Ofcom how to interpret and implement the new requirements, and whether in some cases an alternative approach to the Code requirements might be appropriate and compliant. This will require an ongoing collaborative approach.

We therefore suggest that Ofcom expands its proposed collaborative approach to the telecoms security framework to create a mechanism by which Providers can discuss with Ofcom (on a bilateral and an industry-wide basis as appropriate) any specific challenges with scope, definition and implementation and any general principles can be shared with industry as a whole to ensure consistency. This is the most efficient means of ensuring compliance. However, Ofcom's approach to compliance in recent years has been not to give specific guidance, and when approached by Providers, Ofcom's response has been to state that Providers need to take their own legal and regulatory advice. We urge Ofcom to embrace the different and more collaborative approach envisaged under the new security framework and supervisory model and create a mechanism under which Ofcom and Providers can work closely together, particularly in the first few years of implementation, to: (a) help answer the many new practical and technical questions raised by the security framework; (b) share that information to ensure a consistent interpretation of the requirements across the whole industry; and (c) ensure Ofcom has an in-depth understanding of the complexity of Providers' architecture and systems, and what it would involve to make changes (including the risk of potential impact to customers). We would welcome Ofcom's view on introducing such a mechanism, as a tangible method to foster collaboration. As currently drafted, no such mechanism is envisaged.

[5] See our response to Consultation question 1

In paragraph 5.17 of the Resilience Guidance, Ofcom states that: *"We strongly encourage providers to discuss with us at an early stage any planned new arrangements that may have significant resilience implications. This early engagement with Ofcom might minimise the risk of any further compliance concerns…"*

We agree with Ofcom. This is the kind of approach we hope Ofcom will take to implementing the security framework as a whole. However, the benefits of early engagement will not be realised if the process of sharing information is one way. On the other hand, if Ofcom can give Providers practical advice on implementation and compliance as part of a collaborative approach and create a mechanism by which general principles and anonymised advice and decisions can be shared across industry, then as Ofcom states in paragraph 5.17 of the Resilience Guidance, it will minimise the risk of additional costs due to mitigations having to be put in place after the event.

Timing of implementation is key to proportionality

We note that the proposed commencement date for the majority of provisions in the Act is expected to be 1st October 2022 and Ofcom plans to issue final Procedural Guidance and Resilience Guidance in Autumn 2022. It is likely, therefore, that we will receive the final Guidance on or around the Commencement Date. This raises practical challenges as Providers will need time to make process, procedural and system changes to comply with the new requirements. Ofcom acknowledges in the introduction to this consultation and in paragraph 3.7 of the Procedural Guidance that over the first few years of the regime Providers will "continue to work towards full compliance" but it is not clear whether this statement only relates to Code requirements in Section 3 (which sets out implementation dates which are after the Commencement Date), or whether it should be interpreted more broadly.

Compliance with all the specific measures set out in the Regulation and Code is more complex for proposed Tier 1 Providers than it is for smaller Providers. We welcome Ofcom's acknowledgement that due to the scale and complexity of many provider's operations it is likely to take time to fully achieve improvement[6]. The size and scale of our networks, services and component systems, the legacy of multiple mergers and acquisitions and the need to review and adapt our many existing security controls, processes, and measures (including supply chain) to comply with the specific requirements of the new Regulation and Code mean that it is time, not necessarily money, larger Providers need to ensure compliance in a way that does not adversely affect availability or customer experience for many millions of customers. Smaller Providers will not face this same complexity or the same scale of risk to customers.

The draft version of the Code was first seen by Providers on 1st March 2022. Until we receive the final Regulation, Code, Procedural Guidance and Resilience Guidance, we cannot be sure of the exact scope and detail of the requirements and therefore cannot finalise our impact assessments and implementation plans for the required procedural and system changes.

[6] Paragraph 3.5 of the Procedural Guidance

We urge Ofcom to acknowledge clearly in the Procedural Guidance and indeed in the Resilience Guidance (where there are changes to the 2017 Security Guidance) that there are multiple obligations within the new security framework (not only those set out in section 3 of the Code) where there is likely to be a journey towards compliance after the Commencement Date and full compliance will take time. We appreciate Ofcom's acknowledgement in paragraphs 3.5 and 3.7 of the Procedural Guidance, but we are concerned that the wording could be interpreted as applying only to Section 3 of the Code (which sets out implementation dates which are after the Commencement Date) and not to the requirements more broadly. To give a specific example, the obligations in Section 2 of the Code have no future date for compliance but we do not believe it would be fair or proportionate for Providers to have to implement all these requirements in full by the Commencement Date.

Principles

In considering the Procedural Guidance and proposed revisions to the 2017 Security Guidance, we would expect Ofcom to have regard to the principles under which regulatory activities should be transparent, accountable, proportionate, consistent, and targeted only at cases in which action is needed. These principles require, in particular, a bias against intervention and a commitment to seek the least intrusive regulatory mechanisms to achieve the policy objectives.

In considering whether the Procedural Guidance and Resilience Guidance comply with these principles, we believe Ofcom should:

- consider the extent to which the proposals increase the costs and the regulatory burden upon Providers
- take into account both the cumulative burden and the impact of these proposed changes upon Providers; and
- ensure that the proposals set out in the Guidance are necessary and proportionate to contribute in a meaningful way to improving security monitoring and the security and resilience of networks and services.

DCMS consultation and impact on response to Ofcom's consultation

Ofcom will be aware that DCMS has been consulting on the Regulation and Code in parallel to the Ofcom consultation. The parallel nature of these consultations has affected our response to Ofcom's consultation, and the final versions of the Regulation and Code may materially affect our response to the Guidance and, in particular, how Ofcom proposes to monitor and enforce the requirements. Does Ofcom propose to consult for a second time after publication of the final version of the Regulation and Code, or at least informally consult industry? If there are material changes to either the Regulation or Code, we believe there should be a second consultation on the Guidance.

Whether or not there is to be a follow-up consultation, we suggest holding several Ofcom-led industry roundtables where issues and concerns regarding interpretation, monitoring and enforcement can be raised and discussed (whilst at all times remaining fully compliant with competition laws).

We support Government's ambition to improve security

We share Government's ambition to improve the security of UK telecoms networks and services and believe that with a limited number of changes, Government can ensure the Code and timing for implementation is proportionate, appropriate and practically achievable for all providers.

We wish to work collaboratively and diligently with you to meet the shared ambition of improving the security of UK telecoms networks and services. We believe a collaborative approach will be essential to interpreting, implementing and enforcing the security framework. The fundamental consideration in devising a robust telecoms security framework that works for Providers, customers and UK plc is that Government, Ofcom and Providers work together on a plan that can be delivered in a way that is technically and operationally achievable and does not undermine our ability to keep delivering world-class connectivity.

we believe it is important to make changes in the right way and at the right time so we can deliver on our shared ambitions. For example, some of the timescales for implementing certain requirements in the Code are simply not achievable in the time available, or in some cases with the available technology.

The climate for Providers is very challenging and the financial constraints that we face, mean that we have to adjust our investment and operational spend on an annual basis. This includes diverting investment to areas where we face existing or new regulatory or public policy obligations or commitments. In practice, this means that Providers will invest less in areas that would have previously been expected or planned. This is the opportunity cost of achieving public policy objectives.

VMO2 Recommendations

We support Ofcom's general approach to the Guidance and recommend that Ofcom should: (a) as discussed above, expand its stated commitment to a collaborative approach in more detail within the Guidance; and (b) amend paragraphs 3.5 and 3.7 of the Procedural Guidance to make clear that it will be a journey towards compliance with the Act, Regulation, Code and Guidance after the Commencement Date, and full compliance is not expected immediately.

Additionally, we would like to work with Ofcom as soon as possible after this consultation closes to ensure:

- we have interpreted the requirements correctly,
- interpretation is consistent across industry and
- discuss plans for implementation.

Given the extremely short timetable for implementation we would welcome both bilateral meetings with Ofcom and industry-wide forums for discussion, led by Ofcom (whilst at all times remaining fully compliant with competition laws).

ANNEX 5: PROCEDURAL GUIDANCE

Consultation question 1: Do you have any comments on our proposed approach to compliance monitoring? [section 3]

How to demonstrate compliance

We note that there is no indication in the Guidance how Providers can *demonstrate* compliance. If Providers collectively understand what evidence will be required to demonstrate compliance this can be included in system and process changes and can be implemented in a consistent manner across the industry. It is unclear from the Guidance what evidence will be required to demonstrate compliance with the Act, Regulation, Code and Guidance as part of Ofcom's information gathering and compliance monitoring and whether this will differ between Providers.

Paragraphs 3.5 and 3.7

In paragraph 3.5, Ofcom states that:

"We recognise that the new framework will require an ongoing compliance journey for providers. Firstly, many providers are likely to need to make significant changes to their existing security practices in order to fully comply with the framework. In DCMS' Supply Chain Review, Government expressed the view that the level of security within the sector needed to be improved and that the new framework would facilitate this. Given the scale and complexity of many providers' operations, it is likely to take time to fully achieve this improvement."

In paragraph 3.7, Ofcom states that:

"A key objective of our monitoring role over the first few years of the regime is to determine if each provider is implementing appropriate measures with sufficient pace, as they continue to work towards full compliance. Where we find areas of concern, we will seek to work with providers to ensure appropriate and proportionate measures are implemented in accordance with the security duties. We expect that this collaborative approach will foster more compliant behaviours and reduce the volume of breaches under the 2003 Act, as well as reducing the need for regulatory investigations."

We welcome Ofcom's acknowledgement in paragraphs 3.5 and 3.7 that the new framework will require an ongoing compliance journey and the scale and complexity of many Providers' operations mean it is likely to take time to fully achieve improvement. As we state in the Introduction, it would be helpful if Ofcom amended these paragraphs to clarify that these principles apply to the security framework as a whole and not only to Section 3 of the Code (which sets out implementation dates which are after the Commencement Date).

We also welcome Ofcom's proposal to take a collaborative approach and urge Ofcom to expand this and use a "collaboration-first" approach as discussed in the Introduction to this consultation response.

As Ofcom will be aware, the Code was first seen by Providers on 1st March 2022. We note further that the Regulation and Code is still in draft form subject to consultation and will not be published in final form until closer to the Commencement Date. It is unclear at this stage what further changes will be made. Until we receive the final Regulation, Code, Procedural Guidance and Resilience Guidance, we cannot be sure of the exact scope and detail of the requirements and therefore cannot finalise our impact assessments and implementation plans for the required procedural and system changes.

In addition, because of the complexity of larger Providers' systems and the potential for changes to adversely affect availability and experience for many millions of customers, the process for designing, delivering, testing and deploying systems and any changes is by necessity a prolonged one. As a result, we do not believe that the proposed timetable for implementation is proportionate, reasonable, or achievable.

If Providers are not able to comply with the security framework due to disproportionate timeframes, this will potentially increase the burden on Ofcom to assess and monitor.

Paragraph 3.8 – 3.10 – Compliance monitoring based on Tiering

As we discuss in the Introduction, compliance with all the specific measures set out in the Regulation and Code is more complex for proposed Tier 1 providers than smaller Providers. We welcome Ofcom's acknowledgment that due to the scale and complexity of many providers operations, it is likely to take time to fully achieve improvement.[7] The size and scale of our networks, services and component systems, the legacy of multiple mergers and acquisitions and the need to review and adapt our many existing security controls, processes, and measures (including supply chain) to comply with the specific requirements of the new Regulation and Code mean that it is time, and not necessarily money, larger Providers need to ensure compliance in a way that does not adversely affect availability or customer experience for many millions of customers, or place unreasonable pressures on precious – and limited – skilled and experienced resource.

We do not believe that basing obligations and timing for implementation on turnover is an appropriate means to determine what measures should apply to which Providers (and when), and turnover alone is not a relevant or proportionate means to reduce the risk of security compromise. A Tier 1 Provider may provide a low-risk service and a Tier 2 or 3 Provider a high-risk service. Each should be risk-assessed, not based on turnover but on the relevant risk.

This is not to say we disagree with Ofcom's approach in paragraphs 3.8 - 3.10. We believe tiering as a concept (based on turnover) might be relevant to the extent it is a factor in how Ofcom prioritise engagement with Providers and we understand why Ofcom would expect to focus its own finite resource to carry out proactive compliance monitoring activities on providers in Tiers 1 and 2.

[7] Paragraph 3.5 of the Procedural Guidance

However, even if tiering was only relevant to help Ofcom prioritise engagement, it still raises questions of interpretation. Many Providers have subsidiaries and associated companies that operate independently and at smaller scale. Using VMO2 as an example, how will GiffGaff as a service provider (which is operated separately and independently but is a wholly owned subsidiary of Telefonica UK) be treated? Would they be considered Tier 1 or treated independently of VMO2?

We believe the compliance monitoring approach for Tiers 1-3 should be risk based, rather than based entirely on turnover, and the monitoring approach, including the process flow in paragraph 3.10, figure 1, should be reassessed on this basis. We also believe a collaborative approach – and in particular regular meetings – will be essential as part of the information gathering process and should be included in the process flow set out in paragraph 3.10, figure 1. We set out our views on this in more detail in the Introduction.

Para 3.13 – Establish tiering

It is not clear why there is to be no oversight of Tier 3 providers at all even though they are still required to comply with their legal obligations. While it is understandable that Ofcom will not propose to give the same level of oversight to Tier 3 providers, to exclude them entirely from any requirement to provide evidence of compliance could indicate to a Tier 3 provider they are not expected to fully comply. It would also present a latent risk for greater harm to customers if a Tier 3 Provider were to expand organically or merge with others without having benefitted from substantive collaboration with Ofcom up to that point.

Para 3.16 – 3.28 – Information-gathering powers

We refer to our comments in the Introduction. Reliance primarily on information requests in the absence of collaboration will not be sufficient, or an effective means of monitoring compliance, and may lead to a disproportionate burden on both the Provider and Ofcom.

Appropriate and proportionate enforcement will require a deep understanding of a Provider's network architecture and systems that cannot be obtained from information requests alone. A collaborative approach throughout the process - and in particular before any information request is issued (in draft or otherwise) - will help to ensure that Ofcom obtains sufficient information about Providers' networks, services and systems to frame the questions from the outset, targeting the information most relevant to assess compliance in the format that the Provider is best able to provide it, which will reduce the need for time-and-people-intensive manual processes. This results in a more efficient process for both Ofcom and Providers, which is essential bearing in mind: (a) current resource challenges (which we discuss below); and (b) that the people who will need to provide this information to Ofcom are likely to be the same people who are being tasked with implementing these multiple new security requirements within very challenging timescales - and without impacting availability or customer experience.

Resource challenges

The option to contract-in required resource in most cases is not practical as they do not have the necessary knowledge of VMO2 systems, and recruitment – even if the right UK candidates can be found – is a lengthy process. Training and familiarisation with any Tier 1 Provider's complex systems and architecture can take a significant amount of time; development of existing resources can take years. The reality is that the productivity of new staff dips significantly compared to experienced staff, even after training, until these people have spent some time in-role gaining practical experience of the various VMO2 systems and processes.

The availability of appropriate skilled resource is a known industry problem that has been raised in discussions with DCMS and NCSC and in Parliament during the Committee stage. Ofcom and NCSC are also currently recruiting many people from the same limited pool of resource as Providers and vendors to support their parts in the oversight process. When giving evidence Lyndsey Fussell of Ofcom stated:[8]

"We have indeed already started to build up our team, and have had some success in recruiting people with experience of network security—from the operators, for example. We do not underplay the difficulty of doing that; I completely agree that those are sought-after resources."

Given these challenges, we are particularly concerned that Tier 1 providers are only given 4 months to respond to information requests when Tier 2 providers (who are likely to have smaller and less complex systems and have longer implementation timescales) are given 6 months. In light of the challenges we highlight above, we disagree that such a difference is appropriate or proportionate and we believe there should be a level playing-field, with Tier 1 and 2 providers both given 6 months.

We note that paragraph 3.19 states "where timescales allow". This suggests that there will be occasions when Providers will not see draft information requests in advance of finalisation due to time pressures, most likely caused by the very challenging timescales set out in the Code. This is neither fair nor proportionate and the absence of any consultation is likely to lead to a disproportionate burden on the Provider, as discussed in the Introduction. We believe this wording should be deleted. Providers should see information requests in draft form unless they are recurring requests in identical format to an earlier final information request.

If time pressures mean Providers will have a shorter period of time to respond, a collaborative approach should be taken to determine what information is necessary, appropriate and proportionate to provide in the circumstances. This is unlikely to be the same information which Providers are capable of providing if given more time.

We had a number of questions regarding how the information-gathering process would work in practice, which we believe would be helpful for Ofcom to answer, preferably in the Guidance to ensure consistency. We set these out below.

[8] https://hansard.parliament.uk/Commons/2021-01-19/debates/56837e38-d948-403e-a7e6-b584cbc5c533/Telecommunications(Security)Bill(ThirdSitting)

1. Is it Ofcom's intention to allocate a dedicated individual or a team to the oversight of individual Providers? We believe continuity of engagement with Ofcom during the first few years is essential because a deep understanding of a Provider's architecture, systems and operations will be vital to successful operation of the supervisory model. It will place a disproportionate burden on the Provider and Ofcom if we find ourselves going over the same ground multiple times with different people.
2. The timing for issuing initial Information requests is unclear. Under para 3.26 it states that allocation of tiering will take 3 months. Is the first detailed information request a sequential or parallel activity to tiering? Could the tiering process take less than 3 months? What is the likely start date for issuing information requests? Is this likely to be 1st October 2022, 3 months later or some date in between? Will it be the same for each Provider?
3. When will Ofcom be meeting with each Provider to agree the oversight approach? What will be required from the Provider to facilitate this meeting? What is the intended output from this meeting and how will it be communicated?
4. We assume from para 3.26 that Ofcom expects to issue two substantial requests per calendar year for Tier 1 providers. Is this correct?
5. What is the likely scope of the first set of information requests? Will it focus only on alignment with the Code deadlines, or will it focus on compliance with the Act, Regulation, Code and Resilience Guidance more widely? Will it seek to establish a general understanding of a Provider's network architecture, services and systems and a Provider's current compliance status?
6. Given the likely complexity of the information requests, we will need a reasonable period of time to review any draft information request. How long does Ofcom propose to give? We do not believe the usual 1-2 weeks will be sufficient in this case and therefore urge Ofcom to expand its proposal to collaborate and take a "collaboration-first" approach. Collaboration is critically important in advance of any draft and final information request.
7. Will Ofcom share an illustrative Information Request to allow providers in each Tier to familiarise themselves with the type of request they may receive?

Paragraph 3.35

Clear guidance is needed from Ofcom as to what type of "reasonable costs" Ofcom may incur when undertaking an assessment. Ofcom should be required to demonstrate value for money and there should be transparency with Providers as there may be alternative and appropriate solutions that we can help Ofcom with if we are approached upfront, rather than Ofcom carrying out the work and then presenting Providers with an invoice for the costs incurred by Ofcom or its appointed third party. Also, if third party consultants are instructed, how will Providers be able to determine if their costs are reasonable? Will they have gone through a tender process, for example? Will there be any means of appeal in the event of a dispute over whether costs were "reasonably" incurred?

Any process to engage a third party should: (a) ensure that the third party keeps information confidential; and (b) consider potential conflicts of interest as many large consultancies are engaged from time to time by Providers.

Would the Provider be expected to engage or commission a third party itself to carry out the assessment?

Paragraphs 3.34 to 3.43 – Powers to assess compliance

In paragraph 3.40 it states:

"… we may, in some circumstances, decide it is appropriate for us to use an assessment notice to inform our assessment of a provider's compliance with their security duties. During the early years of the framework, while we are conducting the programme of s135 information notices set out above, we are not planning routinely to use assessment notices."

We welcome the statement that Ofcom does not plan to routinely use assessment notices but would appreciate further clarity on the circumstances in which Ofcom envisages it will use this power.

Consultation question 2: Do you have any comments on our proposed approach to testing? [section 4]

The legal status and benefit of TBEST is unclear and this creates uncertainty and reduces the incentive to participate, which is not what either VMO2 or, we assume, Ofcom wants to achieve.

Under Regulation 14 of the Regulation, Providers will be required to carry out regular testing for the purpose of assessing the risk of security compromises occurring in relation to their network or service, in a manner similar to TBEST.

Ofcom states that: *"we will continue to run TBEST as a voluntary, open, and collaborative program with providers. However, where appropriate, we may exercise our statutory powers to require a provider to undergo testing, either like TBEST or some other types of testing."*

As a result, we are unclear what is the benefit or legal status of TBEST. Ofcom also states that: *"We would expect that it is less likely that testing under s105O will be required if a company undertakes periodic voluntary TBEST"*. However, Providers have no assurance that having gone through TBEST, as well as implementing all the mandatory requirements in the security framework, we will not be required by Ofcom to test again, and differently.

Without clarity on the benefit of TBEST, which is documented in the Guidance, Providers will question the value of carrying out this voluntary process. Given that Regulation 14 is mandatory, each Provider will by necessity focus on compliance with this obligation and senior management will want to understand what additional benefits a voluntary scheme such as TBEST will bring. There would be a clear benefit to Providers if, for instance, we could use TBEST to demonstrate compliance with Regulation 14. But that does not appear to be the case. This is an example of a wider concern we have identified. It is not clear from the Regulation, Code or the Guidance how exactly a Provider should *demonstrate* compliance with its obligations.

Put another way, on the assumption that a Provider can demonstrate that it complies with the mandatory testing requirements under Regulation 14 of the Regulation and the corresponding measures in the Code, under what circumstances would Ofcom deem it appropriate to request further testing? Would the answer differ if a provider had or had not participated in the voluntary TBEST scheme?

Consultation question 3: Do you have any comments on our proposed approach to enforcement? [section 6]

We largely support the approach to enforcement and in particular we agree with the statement in paragraph 6.2 that: *"It is also important that we take action in an efficient and effective way, that is evidence-based, proportionate, consistent, accountable and transparent, and targeted only at cases where action is needed."*

Especially during the early years of implementation, we believe that enforcement would be disproportionate and believe Ofcom should take a "collaboration-first", independent and pragmatic approach. We highlight again the statements in paragraphs 3.5 and 3.7 and our proposal to clarify these statements as set out in the Introduction. We believe this is critical to a reasonable and proportionate implementation.

The power to require 'interim steps' should be exercised with extreme caution and will require the input of subject-matter experts within Ofcom with a clear understanding of a Provider's architecture and systems to understand whether those steps are proportionate, appropriate and reasonable, and what the impact of those steps would be on availability, functionality, performance and customer experience. We strongly advocate a collaborative approach prior to the formal steps set out in section 105U and 105V, and that any proposal to require interim steps is discussed with the Provider in advance.

We note also at paragraph 6.16 that Ofcom may, at any time, revoke or *"vary a direction to make it less onerous (section 105(V)(8))*". Ofcom will be aware that varying a direction may not in practice make the direction less onerous to implement and any variation should be treated as if it was a new proposal and discussed with the Provider so that any practical challenges to implementation can be identified and assessed.

We note that Ofcom proposes to review and consult on updated Enforcement Guidelines in light of the new powers introduced under the Act and has now published this consultation[9]. Does Ofcom have any similar proposals to review the Penalty Guidelines referred to in paragraph 6.8 and 6.25?

Consultation question 4: Do you have any comments on our proposed approach to reporting security compromises? [section 5]

Paragraph 5.2 – 5.8 – Duty to inform users of risk of security compromise

[9] Consultation: Ofcom's approach to enforcement – revising the Regulatory Enforcement Guidelines - Ofcom

This is an entirely new obligation and the circumstances ***when*** a Provider must notify, ***who*** they must notify and ***what*** they must notify are unclear. We recommend that Ofcom sets up an industry roundtable to discuss this to ensure we implement this in a consistent manner across the industry and agree how to address the confusion that such notifications are likely to cause to customers. At the moment there are still a number of unanswered questions and concerns.

Section 105J of the Act refers to notification where there is a "significant risk" of a security compromise occurring. So unlike GDPR and PECR[10] notifications, there may be no actual security compromise (or impact) identified at all, only a risk of one occurring.

Section 105J of the Act refers to those users who *"may be adversely affected by the security compromise"*. We may not know who they are. Is this intended to require us to notify only our own customers, or is it expected we should identify and notify other users? There are very real practical challenges of doing this. We believe the notification requirement should be limited to our customers, except to the extent that Providers share information in accordance with Regulation 15.

As Ofcom rightly points out, providers are likely to be aware of many "potential vulnerabilities" within their networks and services. However, the guidance in paragraph 5.3 is potentially open to interpretation, in particular this statement:

"where providers have reasonable grounds for believing that a vulnerability within the network or service is unlikely to result in an actual security compromise, or even if it did, it would be unlikely to have an adverse effect on users."

We assume that a Provider must not satisfy both limbs of this test. For example, using a risk-based approach, if the vulnerability would have a high impact on users if a security compromise occurred but there was low likelihood of a security compromise occurring (due to firewall settings around the vulnerable system, for instance) we assume that there would be no requirement to notify. Is that the correct interpretation?

Even if narrowed down in this way, the obligation to notify based on risk rather than actual security compromise is new and as stated above, we recommend that Ofcom sets up an industry roundtable to discuss this to ensure consistent implementation.

In paragraph 5.6, the reference to *"where no measures exist, but the user could mitigate the risk to themselves by moving to another provider"* is concerning. This particular factor does not appear in section 105J of the Act but appears to be an interpretation taken by Ofcom for the purposes of the Procedural Guidance. We urge Ofcom to remove this bullet point. If it remains in the Procedural Guidance, Ofcom and Providers will need to exercise extreme caution in the pursuit of this as there is potential for it to cause great confusion to consumers, serious reputational and commercial damage to Providers and has the potential for abuse by other Providers, especially given there are no clear

[10] Privacy and Electronic Communications (EC Directive) Regulations 2003

parameters as to exactly when notifications to users should be sent, resulting in an inconsistent approach.

The wide-ranging definition of 'security compromise' also creates confusion and complexity. The obligation in S105J of the Act appears aimed at 'cyber-security' incidents but in theory could include risks to 'availability' or other 'performance' metrics. We discuss the problems and confusion this creates below in response to paragraphs 5.9-5.36 and again in response to Consultation Question 9. It would be helpful if Ofcom included further guidance on the type of incidents this requirement is intended to capture, and which ought to be notified to users. We believe examples would be useful.

Paragraph 5.9 – 5.36 - security compromise reporting to Ofcom

The reporting obligations are similar to the ones included in the 2017 Security Guidance with some expansion of the reporting obligations. They appear to focus on 'availability' metrics and are generally well-understood in this context. However, the obligations and metrics do not easily translate to other 'security compromises'. We believe further discussion with Ofcom (as an industry and in bilateral meetings as appropriate) is needed and further guidance is required to enable Providers to understand exactly which 'security' (rather than 'availability') incidents must be reported – and how.

Sensitive cyber-security incidents cannot be notified by email and we recommend that we set up a separate secure reporting mechanism for security incidents and the Procedural Guidance clearly splits out reporting obligations into: (a) availability incidents; and (b) cyber-security incidents that may or may not affect availability. The qualitative criteria and numerical reporting thresholds and the template provided in A3 (which is the same as the template in the 2017 Security Guidance) apply to 'availability' incidents and do not easily map to other 'security compromises'.

Much of the problem stems from the catch-all nature of the definition 'security compromise', which in theory could catch incidents as wide ranging as cyber-security incidents (such as DDoS or unauthorised access, regardless of scale or impact), single data breaches by call centre agents and minor degradation of performance caused by the use of contention in a network (given it may affect speed at peak times, and therefore performance, compared with quiet times). This is unhelpfully wide, stretches the natural meaning of 'security compromise' to breaking point and places the burden on Ofcom and Providers to interpret obligations relating to 'security compromise' in a pragmatic, appropriate and proportionate manner.

We understand that a total loss of service (an 'availability' incident) is clearly a security compromise that must be notified to Ofcom if it meets the qualitative or quantitative metrics set out in the Procedural Guidance. This is well-understood. However, if there is a cyber-security incident (regardless of severity), or a 'performance' issue other than 'availability' (such as a drop in speed or throughput), or if a resilient link were taken out of service for maintenance (but the service remained unaffected) it is not clear whether (or when) Providers must report to Ofcom under the Procedural Guidance in the absence of any impact on 'availability'.

As we state above, we recommend that Ofcom:

- break down the definition of 'security compromise' into different categories and create a separate set of criteria and template for reporting 'cyber-security' incidents which fall within s105K(1)(b) of the Act but do not affect 'availability'; and
- arrange an industry roundtable to clarify which 'security compromises' are important and proportionate for Providers to report to Ofcom – and which risks of security compromise should be notified to users.

Under paragraph 5.25, providers must keep data for security compromises that have been reported for no less than 18 months following incident resolution. We note that this is more than the storage requirement set out in the Regulation (13 months). We interpret this requirement as meaning data which was collated for the purposes of incident reporting and further discussion with Ofcom, which we would keep for 18 months, but not the underlying data stored in network systems. It would be helpful if Ofcom could confirm this interpretation.

In paragraph 5.26 Ofcom refers to section 105K(2), under which providers must take account of a number of factors in determining whether the effect of a security compromise is significant for the purpose of complying with their reporting obligations. Some pragmatism will be required here, particularly in relation to s105K(2)(d), which refers to *"the extent to which activities of persons who use the network or service are or would be affected by the effect on the operation of the network or service."* Except in the most obvious of cases, such as services provided to 'blue light' organisations which are used to provide access to emergency services, this is extremely difficult for Providers to determine. Providers do not monitor activity in this way and have not done so since the introduction of the Open Internet Regulation[11] – and increasing use of encryption makes this an even greater challenge. Customers may be using a myriad of OTT Cloud and App based applications but to identify these for each customer and whether (and if so, to what extent) a customer is dependent upon them is not something we have the technical capability to do. An obligation to obtain this information, for example at point of sale, would be impractical, disproportionate and any information is likely to quickly become out of date.

Paragraph 5.36 (and 2.17) refer to Ofcom's periodic reports to the UK Government such as the Connected Nations report. These reports must now include an annual summary of the security compromises which have been reported to Ofcom.

There are two key concerns here:

- **Security and availability incidents are likely to be sensitive.** Will Providers be identified? If not, will the information be sufficient to identify a Provider? What is the process by which a Provider can object to the publication of confidential information? Due to the sensitive nature of the information, the potential for reputational damage and the potential for misuse by 'bad actors', it will be necessary for Ofcom to ensure that the granular details are not disclosed. We would welcome a discussion with Ofcom to understand how it proposes to report these incidents.

[11] Regulation EU 2015/2120

- **When will this commence?** Is this expected to be included in the 2022 Connected Nations report, if published after the Commencement Date? We recommend that, if possible, as with the security reports (referred to in paragraph 2.16), this should commence from 2024, 2 years from the Commencement Date.

Annex A1 to A3 - Qualitative criteria and thresholds for reporting security compromises

We state above our concern that the qualitative criteria and thresholds do not help to identify what is a 'major cyber security breach' and which 'security' incidents Providers should report to Ofcom. The criteria are largely applicable to 'availability' reporting and do not easily translate to 'security' incidents as defined by the Act. We recommend that Ofcom break down the definition of 'security compromise' into different categories and create a separate set of qualitative criteria and template for reporting 'cyber-security' incidents which fall within s105K(1)(b) of the Act.

A1.1 Urgent security compromises

We note the inclusion of the following new line in the "urgent" security compromises category: *"Any single security compromise that affects the provision of wholesale services to both fixed and mobile communications providers"*. We are unclear what this means in practice, particularly in terms of the scale of the impact required for it to become an urgent incident. Some examples, or a numerical threshold might be helpful in this context.

We understand that a total loss of service (an 'availability' incident) is clearly a security compromise that must be notified to Ofcom if it meets the qualitative or numerical metrics set out in the Procedural Guidance. This is well-understood. However, if there is a partial loss of service, or a cyber-security incident, or a personal data breach, or a 'performance' issue other than 'availability' (such as a drop in speed or throughput), or if a resilient link were taken out of service for maintenance (but the rest of the service remained unaffected) it is not clear whether (and in what circumstances) Providers should report to Ofcom under the Procedural Guidance and whether (and in what circumstances) any of these issues would become an urgent incident. We urge further clarity on this with some practical examples set out in the Guidance.

A1.3 General - Data breach reporting

We have raised this issue with Ofcom before in relation to the 2017 Security Guidance and it is now more pressing given the very significant overlap between what is a 'security compromise' and what is a personal data breach reportable to (and enforceable by) the ICO. Under this section, a reportable security compromise includes any security compromises reported to other Government agencies or departments. In theory this could turn a single personal data breach report to the ICO into a reportable 'security compromise'. We do not believe that dual-reporting all these incidents to the ICO and to Ofcom is proportionate or indeed what Ofcom is trying to achieve through paragraph A1.3.

Under our current reporting process, we will forward to Ofcom any significant data breaches reported to the ICO for Ofcom's awareness, but as agreed with Ofcom in discussions relating to the 2017

Security Guidance we do not currently report small-scale data breaches we have reported to the ICO. This reduces the burden on Ofcom and on the Provider. We need clarification regarding what data breaches we must report to Ofcom and how Ofcom proposes to work with the ICO in relation to investigation and enforcement of personal data breaches.

Numerical thresholds

We note that Ofcom has removed the Broadcast network numerical thresholds. Can Ofcom explain why it has done this and whether it expects security compromises relating to TV services to be reported under the new Procedural Guidance?

The remainder of our comments largely relate to mobile incident reporting. In particular, we note that the following language included in the Mobile network numerical thresholds set out in table 2 and note 5 in para 4.18 of the 2017 Security Guidance has been removed:

- **"MNO voice or data service/network offered to retail customers. See notes"**
- **Note 5:** ***"****Due to the complexity of mobile networks and the inherent difficulty in determining the exact number of end customers affected by an incident, Ofcom has agreed a reporting process with each of the four UK mobile operators which is based on their individual definitions of a major service failure (MSF). Network MSFs are incidents which have a significant impact on the network and are raised to senior management within the MNO. The exact details of an MNOs MSF criteria are commercially sensitive so will not be discussed here. The ultimate intention is to ensure reporting of mobile incidents which cause similar levels of customer disruption to those reportable on fixed networks. At the time of publication of this guidance, we are still in discussions with MNOs about revising these agreements, in order address the concerns about the current levels of reporting which we set out in our June 2017 consultation. In summary, the revised agreements are intended to result in more consistency between MNOs in reporting and in the calculation of customer impact, which for most MNOs will represent a significant increase in the number of incidents they report".*

This raises the question, what should MNOs report? We are not sure why MNO reporting has been deleted from the table and the explanatory note removed. No explanation has been given. VMO2 has an agreed reporting process for mobile incidents with Ofcom. What is the status of this agreement and what exactly should VMO2 (as an MNO) be reporting under the new Procedural Guidance? We would welcome a meeting with Ofcom once the consultation has closed to discuss what in practice ought to be reported and urge Ofcom to clarify an MNO's reporting obligations in the Guidance.

Paragraph A2.10 – loss of technology

This suggests that a loss of a single technology that does not affect availability of service (for instance loss of 3G when 4G remains available or loss of 'VoWifi' when 3G and 4G remains available) must be reported. This is a new provision and the scope and rationale for reporting is unclear. As discussed above, we would welcome clarity on the exact reporting obligations for an MNO. We believe this obligation should be removed. If Ofcom proposes to retain this new obligation, what is the rationale

for doing so and what is the qualitative and numeric threshold and how should customer impact be calculated?

A2.10 and A2.11 seem to suggest that loss of a single cell site will be reportable, which would be a new requirement and we do not believe such an obligation is proportionate. Can Ofcom clarify the threshold and rationale for reporting incidents where one or more cell sites are unavailable?

Paragraph A2.14 2.19 – Number/proportion of users affected

Under paragraph A2.17, the Procedural Guidance states: *"Where exact numbers are not available (for example due to a mobile cell site failure), we expect the provider to use historical data to estimate the number of end users affected."*

what historical data is relevant to estimate number of customers affected by a mobile incident when the actual number cannot be determined? We would welcome further clarity on this.

We have similar issues on the fixed network in identifying number of customers affected, where a core transmission issue or a peering issue has led to some websites or services not being available for a subset of customers, but there is no overall loss of service. Generally, we can use traffic data volumes to show any reduction and movement of internet traffic data across the network but that does not give an indication of number of customers affected. We would appreciate further discussion with Ofcom on what information would be possible and proportionate to provide and would be useful to Ofcom.

Consultation question 5: Do you have any comments on our proposed approach to information sharing? [section 7]

Ofcom's approach to confidentiality to date has given Providers confidence and assurance that data will be kept secure. Sharing data with third parties has generally been done with a Provider's prior knowledge and consent and gives Providers the opportunity to: (a) understand who has access to the data; and (b) ensure that the third party understands its sensitivity and does not disclose it. This approach has been very much appreciated by VMO2.

The new security framework introduces many new – and sensitive – gateways to sharing information with third parties. Information shared in relation to the security framework is likely to be particularly sensitive and could be very damaging if disclosed, for customers, the Provider and potentially for UK plc. We would prefer to see paragraph 7.7 amended so that "Where appropriate, Ofcom may seek consent" is changed to "Where appropriate, Ofcom will seek consent".

Our concern is to ensure that any third party with access to this sensitive data understands its sensitivity, that it should be kept confidential, and the impact should it be disclosed.

If Ofcom uses its power under section 105L to notify other parties including other Providers of a potential security compromise, extreme caution will need to be exercised given this has wide ranging

potential implications – not least from a competition perspective. In addition, the information will certainly be considered commercially sensitive given the impact it may have on financial markets, the reputational impact on a Provider and the impact on customers if leaked.

Consultation question 6: Do you have any other comments on our draft statement of general policy set out at Annex A5 to this consultation?

Para 2.15: Under section 105Z (reports on security) Government has the right to publish Ofcom's security reports or extracts from them. Will Providers have sight of what Ofcom intends to report to the Secretary of State prior to its submission? If yes, how long before and do Providers have a right to appeal the submission content? We are also concerned that the Secretary of State may not know what information is sensitive and confidential and therefore should not be published (s105Z(7)). Government will also be subject to freedom of information requests even if the report is not published. We would welcome discussion with Ofcom in advance of sending a security report to the Secretary of State so that any sensitive and confidential information is either redacted, anonymised (in a way that cannot be reverse engineered) or clearly marked as confidential.

Para 2.18: The Procedural Guidance refers to an Information Sharing Gateway between DCMS and NCSC. Given the sensitivity of the information that will be shared (including future plans as foreseen in para 3.17) there is a need to ensure the gateways are secure and all those having access are made aware of the sensitivity of the information and that it should not be disclosed. Although Section 7 discusses information sharing it does not address the security of those gateways.

Under Section 105W of the Act, Providers are subject to civil liability for breach of its statutory duties. S105W(6) states that the consent of Ofcom is required for the bringing of proceedings by virtue of this section and s105W(7) states that if Ofcom gives consent subject to conditions relating to the conduct of the proceedings, the proceedings are not to be carried on except in compliance with those conditions.

We note that the Procedural Guidance makes no reference to this and gives no indication of when Ofcom is likely to give consent or what conditions it may impose. We would have expected to see this referred to in the Procedural Guidance. Is Ofcom intending to give any guidance on this?

ANNEX 6: DRAFT RESILIENCE GUIDANCE

Introduction

Overall, we agree with Ofcom's approach to the Resilience Guidance and believe it is appropriate and proportionate, but we have some specific practical, technical and operational comments on the detailed provisions which we set out below.

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?

Paragraphs 4.13 – 4.16

We are unclear as to the legal status of the various sources of further advice and best practice referred to in the Resilience Guidance, most notably those referred to in 4.13 to 4.16. Ofcom states in paragraph 4.12 that *"we will expect providers to consider where relevant to their operations." And "these documents do not themselves form part of the guidance provided by this document".*

These sources of best practice will be considered by Providers, but it is not clear whether (and if so to what extent and when) compliance will be expected, and to what extent Ofcom will require Providers to clearly document and explain why a Provider may have deviated from this advice and best practice in particular cases, much as it can do under s105I in relation to the Code. This needs to be clarified. This is an example of our wider concern regarding how we demonstrate compliance.

In relation to ND1643 we note that protection is only as strong as the weakest link and is reliant on the Provider at the other end of the link also implementing ND1643, so that we protect each other on a reciprocal basis. Individual implementation by one Provider offers no protection and would be wasted cost.

As with ND1643, ND1653 only benefits a Provider if the Provider at the other end of the link implements the same, so that we protect each other on a reciprocal basis. It is essential that before such a mechanism is deployed in earnest in the UK network that Providers carry out validation of non-functional/functional behaviour of this dynamic and adaptive mechanism in a captive lab environment and then introduce into the network in a controlled manner to make sure there are no further issues encountered in a live environment.

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?

Again, we believe most of the Guidance in this section is proportionate and reasonable.

Paragraph 5.4

We agree the questions remain helpful to establish accountability and expertise, but we believe that Ofcom should acknowledge that there may be more than one owner of resilience matters, including at Board level (which we assume to mean Executive Committee level, not shareholder level). Any company that has a separate CIO and CTO may have more than one person within the organisation, even at Board level, who is responsible for resilience matters relating to different parts of the network infrastructure.

Paragraphs 4.13 - 4.16 and paragraph 5.13

Under paragraph 5.13 Providers are expected to keep abreast of the range of resilience related guidance, best practice and standards (such as those referred to in paragraphs 4.13 – 4.16). These best practice documents are likely to be subject to change on a more regular basis than the Guidance. This can clearly be taken into account in relation to new projects but is Ofcom expecting that Providers re-architect existing networks and services and change projects in-flight to take account of any changes to best practice? Or can a Provider take a risk-based approach to any changes to best practice? Again, this raises the question of how Providers can demonstrate compliance.

Paragraph 5.17

Ofcom states that: *"We strongly encourage providers to discuss with us at an early stage any planned new arrangements that may have significant resilience implications. This early engagement with Ofcom might minimise the risk of any future compliance concerns, and the associated risk that additional costs will need to be incurred as a result of mitigations having to be put in place after the event."*

We agree with this statement but as we set out in the Introduction to this consultation response, we believe that collaboration is essential. The benefits of early engagement will not be realised if the process of sharing information is one way. On the other hand, if Ofcom gives Providers practical advice on implementation and compliance as part of a collaborative approach and creates a mechanism by which general principles and anonymised advice and decisions can be shared across industry, then as Ofcom states in paragraph 5.17 of the Resilience Guidance, it will minimise the risk of additional costs due to mitigations having to be put in place after the event.

Paragraph 5.20

We agree with the general statement and intent but we are concerned how we would demonstrate compliance. What is "sufficient" and how is a Provider able to determine "sufficiency"?

Paragraph 5.22 – 5.23 – risk assessment and provision of information

Paragraph 5.23 states that *"The risk appetite of end users will vary, so we expect providers to provide information about the resilience of their services to allow customers to make informed purchasing choices."*

This is a new obligation which is not in the Act. We are unclear why this new obligation is appropriate or proportionate to impose, particularly in relation to consumer fixed and mobile services. What does this mean in practice? We need additional clarity on what is expected in order to comply. What information is Ofcom expecting Providers to give to its customers (and potentially other end users)? Is Ofcom expecting Providers to give overall percentage (%) availability statistics or some other metric, for instance relating to quality of service rather than resilience/availability? If so, what is this? How should it be provided? On a Provider's website or a mandatory part of the customer sales journey, for example in the way that speed information must be given at point of sale in accordance with the Broadband Speed Code?

If Ofcom expects additional information to be provided at point of sale, this will require system changes. Is Ofcom expecting full compliance with the Guidance as a whole by the Commencement Date? It will not be technically or practically possible to make system changes and thoroughly test and implement them by the Commencement Date. We set out more detailed comments about timing for compliance in the Introduction to this consultation response.

Paragraph 5.23 goes on to state: *"Providers should attempt to match the delivered network and service availability and performance levels to the customer expectations that have been set"*. We are not clear how we do this in relation to a standard consumer service or indeed how those consumer expectations 'have been set' other than through our own marketing material and terms and conditions. Is that sufficient? Customers may have other expectations, but we can only provide the service we are advertising and as described in our terms and conditions. Can Ofcom explain how it expects this requirement to apply in practice and give some examples?

Paragraph 5.27 – ND1653

We refer to our comments in response to paragraph 4.16.

Paragraph 5.31 – 5.34 – public access to emergency services

Although we agree in principle with the requirements in this section, we need additional clarity on exactly what is expected, appropriate and proportionate in order to comply. In particular, paragraph 5.33 states that BT "has developed a set of test call handling procedures. We expect to publish an outline of these procedures on Ofcom's website in the future." To comply, we need a copy of these test call handling procedures as soon as possible so we can begin work to amend our internal processes.

Are these obligations to commence on the Commencement Date?

Paragraph 5.46

In managing risk of loss of power, other government policy linked to ESG measures may have an impact on Providers. This includes a move to NetZero and potential withdrawal of diesel fuel for generators. At this point it is unclear what this would mean for Providers and is an industry-wide issue that should be discussed.

Consultation question 9: Do you have any other comments on our draft guidance set out at Annex A6 to this consultation?

How to demonstrate compliance

One of the key concerns we have in relation to the Resilience Guidance – and indeed the Guidance as a whole – is how to demonstrate compliance. We refer to this in several parts of our response. In the absence of specific metrics, it is difficult to understand how Providers will demonstrate compliance. We would welcome additional clarification in the Guidance.

Definition of 'security compromise'

The definition of 'security compromise', as we state in response to consultation question 4, is problematic because the actual definition has been stretched so far from its natural meaning that it catches many disparate circumstances and causes confusion. Technical colleagues have also raised concerns with the definition of 'security compromises' related to the resilience of networks used throughout the Resilience Guidance. Strictly speaking 'availability' is a performance metric – along with other parameters like latency, speed etc. We would welcome clarity as to what metrics, as part of 'performance' (which is included within the definition of 'security compromise') we are being policed against.

We understand that a total loss of service (an 'availability' incident) is clearly a security compromise that must be notified to Ofcom if it meets the qualitative or numerical metrics set out in the Procedural Guidance. That is well-understood. However, if there is a partial loss of service, or a cyber-security incident, or a personal data breach, or a 'performance' issue other than 'availability' (such as a drop in speed or throughput), or if a resilient link were taken out of service for maintenance (but the rest of the service remained unaffected) it is not clear whether (and in what circumstances) Providers should report to Ofcom under the Procedural Guidance and whether (and in what circumstances) any of these issues would become an urgent incident. We urge further clarity on this with some practical examples set out in the Guidance.

Governance and improvement

In terms of governance and improvement, we believe it would be helpful to set up a best practice industry group or possibly an NICC standards task group to support Providers with delivery and governance against the requirements. The existing best practice groups are focussed on their own guidance – it would be helpful to have an industry group that looked at all best practice relevant to a

Provider in complying with the Act, Regulation, Code and Guidance (whilst at all times remaining fully compliant with competition laws).