Statement on Network and Service Resilience Guidance

Guidance for communications providers on resilience-related security duties under the Communications Act 2003

Statement

Published 6 September 2024

Contents

1. Overview

Resilient telecoms networks are vitally important to consumers and businesses across the UK, given our increasing reliance on digital communications services to stay connected at home, at work, and on the move.

As more of our economic and social activities shift online in the years ahead, and technological innovation continues to deliver new products and services at rapid speed, it is crucial that the telecoms networks that underpin them are sufficiently resilient to meet increased societal demands. The consequences of network outages are likely to become more severe as society becomes increasingly dependent on networks to function.

In order to strengthen the security and resilience of UK networks and services, a new framework came into force in October 2022[1] which imposed various duties on providers of public electronic communications networks and services (PECN/S). To provide greater clarity on how such network and service providers can comply with their security duties in respect of network and service resilience under this framework, we have decided to update our resilience guidance.

Our updated Network and Service Resilience Guidance for Communications Providers (the Guidance), summarised in Sections 4-7 of this document, describes a range of practices in the architecture, design, and operational models that underpin robust and resilient telecoms networks and services, as well as more specific measures that we expect providers to consider.

These are designed to help achieve our aim of ensuring an appropriate level of resilience for networks and services across the UK. The Guidance takes a principles-based approach to resilience and has a broad application. It is designed to be flexible enough to apply to all types of PECN/S.

What we have decided – in brief.

We are introducing an updated version of our resilience guidance for providers of PECN/S, which sets out measures we expect them to take in relation to the resilience of their networks and services as part of their security duties imposed by and under s105A-D of the Communications Act 2003.

These measures include:

- ensuring that networks are designed to avoid or reduce single points of failure;
- ensuring that key infrastructure points have automatic failover functionality built in so that when equipment fails, network traffic is immediately diverted to another device or site that can maintain end user connectivity;
- setting out the processes, tools, and training that should be considered to support the requirements on resilience.

[1] The new duties are found in the Communications Act 2003 as amended by the Telecommunications (Security) Act 2021, and supplemented by the Electronic Communications (Security Measures) Regulations 2022.

Next Steps

This Statement follows a consultation published in December 2023 that sought views on proposed guidance. Providers are now expected to have regard to the Guidance when considering their resilience-related security duties.

Alongside the consultation, we published a Call for Input (CFI) on power backup for mobile radio access networks (RAN). Our aim was to prompt a discussion about what power backup mobile network operators (MNOs) can, and should, provide for their networks and services. We have published the responses to this CFI so interested parties can consider the views shared by respondents.

While the feedback showed strong interest in mobile resilience, some highlighted the need for a broader approach to power backup beyond the telecoms sector. Additionally, responses offered valuable insights into potential harms from power outages, such as the effect on emergency services and communication difficulties, particularly in rural areas where communities could be more vulnerable to the impacts of outages.

Over the coming months, we will further analyse the information gathered to determine if additional resilience measures are needed for the mobile RAN. This analysis will consider a range of solutions, rather than a one-size-fits-all approach, and we plan to work with government and industry to identify the most suitable way forward.

2. Background

Summary

2.1 This section provides an overview of network resilience, its growing importance, and Ofcom's goals in this area.

2.2 In later sections, we discuss in detail why it is important for providers to consider their statutory duties regarding resilience, and we explain how we have concluded on a particular set of resilience measures in the Guidance.

What is network and service resilience?

Resilience is the ability of a network or a service to resist disruption from a range of causes

2.3 Threats to the operation of a network or service include but are not limited to:

a) Physical threats or shocks such as fire, vandalism, or flooding and other extreme weather events;

b) Technology vulnerabilities that result from hardware and software failures or capacity/overload problems;

c) Human error that results from inadequate training/ recruitment or negligence;

d) Architecture design failings, for example when networks are subject to a single point of failure and do not have backup routes or systems available when things go wrong.

2.4 Resilience is the ability of a network or a service to resist disruption from a range of causes. We interpret resilience in the broadest sense as the ability of an organisation, resource, or structure to be resistant to a range of known and future internal and external threats, to withstand the effects of a partial loss or degradation of platform, system, or service, to recover and resume service with the minimum reasonable loss of performance, and adopt lessons learnt from any incidents.

2.5 As reflected in the EC-RRG[2] Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure[3], resilience can be seen to include:

a) Good network design;

b) Effective operational processes for network operations, management, and maintenance;

c) Appropriate processes to respond to a range of contingent risks;

d) Business continuity planning and disaster recovery; and

e) Appropriate review processes of previous incidents.

[2] The Electronic Communications Resilience & Response Group (EC-RRG) is a cross government and telecoms industry forum whose aim is to ensure the telecoms sector remains resilient to threats and risks to services.
[3] Electronic Communications Resilience & Response Group, 2021. *Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure*

Ensuring appropriate network resilience has never been more important

Consumers and businesses are heavily reliant on these networks and services

2.6 For most people in the UK, being online is now a major part of daily life. Ninety-three per cent of adults have internet access at home and the increase in the availability of fast and reliable home broadband, combined with widespread smart phone ownership, has significantly changed the way that we interact with the world.[4]

2.7 People now access a wide and increasing range of online services across PECN/S. This includes gaming, banking, remote working, ecommerce, video-on demand/streaming, as well as government services.

2.8 The growing shift to online services has led to a considerable increase in demand for fixed and mobile data in recent years, with adults spending an average of three hours and 41 minutes a day online.[5] [6] As a result, we have become reliant on digital communications as a society, with nearly all (94%) UK adults using an online communications service for making voice/video calls or sending messages in 2022.

2.9 In contrast, outgoing landline calls fell by 20% year on year, and outgoing mobile calls fell by 9% over the same period. Despite this decline, the total volume of outgoing calls from fixed lines was 32 billion minutes and 170 billion minutes for mobile in 2022.[7] These figures highlight how these remain important methods of communication even as new technology is adopted.

2.10 This is also a trend occurring in media consumption habits. On average, people watched about 16% less broadcast TV between 2019 and 2022 as take up of subscription video-on-demand services rose from 47% of households to 66% over the same period.[8] In addition, online gaming is now played by 38% of adults and 57% of children.[9]

2.11 There is also much more dependence on access to digital services to carry out essential day to day tasks. In banking, almost nine in ten (88%) adults with a day-to-day account banked online or used a mobile app in 2022, and in retail nine in ten (90%) people said they had made an online shopping purchase in the last 12 months.[10] [11] In addition, around one in five (22%) people in the workforce work at least one day from home, and around one in eight people work from home exclusively.[12]

2.12 Cloud computing, which is underpinned by telecommunication networks, is also being rapidly adopted by businesses across the economy. The UK cloud infrastructure market is growing, with overall revenues increasing at a rate of 35% to 40% annually in recent years.

---

[4] Ofcom, 2023. *Communications Market Report 2023*

[5] Ofcom, 2023. *Communications Market Report 2023,* p1: 'The average consumption per data user on mobile increased by 24% in 2022 to 8.0 GB per month. On fixed broadband connections, the average monthly data use increased by 6% to 482 GB.'

[6] Ofcom, 2023.*Online Nation 2023*, p12.

[7] Ofcom, 2023. *Communications Market Report 2023*

[8] Broadcast TV: Barb 28-day consolidated, TV sets only. Subscription video-on-demand: Barb Establishment Survey Q1 2019 and Q1 2023.

[9] Ofcom, 2023. *Online Nation 2023.*

[10] Financial Conduct Authority, 2023. *Financial Lives 2022*

[11] DESNZ, 2023. *DESNZ Public Attitudes Tracker: Consumer Issues Spring 2023*

[12] UK Parliament, 2022. *The impact of remote and hybrid working on workers and organisations.*

Ofcom estimates this market generated revenues of £7.0bn to £7.5bn in 2022.[13] As a result, the cloud has become an essential part of how many of these online services are delivered, including gaming, banking, remote working, e-commerce, and video on-demand/streaming.

2.13 Both mobile and fixed networks play a critical role in the event of an emergency. 41.9 million 999/112 calls were made in 2023, of which 79% were from a mobile and 15% from a landline.[14]

2.14 In March 2023, the UK Government launched its Emergency Alert service, which was then trialled in April 2023. It is designed to warn people if there is a danger to life nearby, in the case of events like severe flooding, fires and extreme weather. Under the system, mobile phone masts in the surrounding area broadcast an alert, with every compatible mobile phone or tablet in range getting the alert, if they are using a device on a 4G or 5G network. In February 2024, the Emergency Alert service was successfully used to notify people in certain parts of Plymouth to evacuate the area due to an unexploded WWII bomb.

2.15 An example of the widespread impact of a network outage was highlighted by a major incident that impacted Australian telecoms firm Optus in November 2023. An outage caused by what Optus described as a 'technical network fault' affected 10 million people for around 12 hours before services were restored. During this period, customers were left without mobile and internet services, and the disruption also spread to transport services and payment systems.[15]

2.16 On 25 June 2023, BT experienced a network fault that affected its ability to connect calls to emergency services for several hours. During the incident, nearly 14,000 call attempts were unsuccessful. Ofcom launched an investigation to establish whether the company had failed to comply with its legal duties to take appropriate and proportionate measures to prepare for potential disruption to its network. We found that BT did not have sufficient warning systems in place for when this kind of incident occurs, nor did it have adequate procedures for promptly assessing the severity, impact and likely cause of any such incident or for identifying mitigating actions. Although there have been no confirmed reports by the emergency authorities of serious harm to members of the public as a result of the incident, the potential degree of harm was extremely significant. As a result of BT's failures, Ofcom has decided to fine the company £17.5 million.[16]

Technology innovations can create opportunities but also pose new risks

2.17 Technological innovation is delivering new services at a rapid rate, and this is transforming the way that telecoms networks are built and operate.

2.18 5G coverage continues to advance, with 93% of premises being able to get a 5G signal outdoors from at least one MNO and 5G data traffic rose from 9% of total mobile traffic in 2022 to 17% in 2023.[17] The UK's MNOs will switch off their 3G and then 2G networks over the next few years and have confirmed to the Government that they do not intend to offer 2G and 3G mobile networks past 2033 at the latest. This will support further roll-out of the 4G and 5G networks which offer faster and more reliable services for customers. The

[13] Ofcom, 2023. *Cloud services market study – Final Report.*
[14] DCMS, HO, DHSC, 2023. *999 and 112: the UK's national emergency numbers*. https://www.gov.uk/guidance/999-and-112-the-uks-national-emergency-numbers [accessed 16 July 2024].
[15] BBC News, 2023. *Optus outage: Millions affected by Australian network failure*.
[16] Ofcom, 2024. *BT fined £17.5m for 999 call-handling failures.*
[17] Ofcom, 2023. *Connected Nations 2023*.

operators are making their own decisions on the timing and process of the 3G and 2G switch-offs, and they all plan to switch off their 3G networks first. Vodafone and EE have now completed their 3G network switch offs in the UK. [18]

2.19 The number of active IoT (Internet of Things) connections on MNO networks, which provide connectivity for smart meters, connected cameras and range of other consumer and industrial devices, stands at more than 24 million, with MNOs' IoT traffic growing by 31% over the last year.[19]

2.20 Apple and Meta have both announced mixed reality headsets, as the immersive technologies of augmented and virtual reality emerge in consumer markets. These allow people to use apps, view content, or interact with others in a way that blends the physical and virtual worlds. In future, this type of technology has the potential to become another regular feature of our lives which will also depend on robust and reliable telecoms networks, particularly given the large volumes of data it consumes.

2.21 As uptake of new services increases, and technological innovation continues, it is important for providers to consider how these developments depend on, and impact, the resilience of their networks/services, and incorporate this into their design and operation going forward.

2.22 The increasing availability of low earth orbit satellite broadband services also offers an option for customers who are unable to otherwise access at least decent broadband speeds from fixed or mobile connections.[20] In 2022, the UK Government launched a trial to see whether satellite can be used to deliver high speed connections in more than a dozen hard to reach locations across the UK. In addition, Apple and Android have both launched emergency communication services via satellite for certain mobile devices. Further development of "direct to device" services from such "Non-Terrestrial Networks" (NTNs) are being explored in standards groups such as 3GPP, and MNOs and satellite operators such as Starlink and AST are moving towards deployments.[21]

2.23 Resilience considerations are particularly important as older technology is phased out. For instance, the current migration of landline customers from PSTN to digital landlines (based on VoIP technology) means that some consumers will become more reliant on mobile networks in the event of a power outage that affects fixed networks or homes, such as in the event of severe storms.

Climate change is leading to more uncertain and severe weather conditions

2.24 Climate change is having an increasingly adverse impact on the UK's critical national infrastructure (CNI), and this is set to "worsen substantially" in the future under all reasonable climate change scenarios.[22]

[18] Ofcom, 2023. *3G and 2G switch-off.*
[19] Ofcom, 2023.*Connected Nations 2023*.
[20] The Government has defined a decent connection as one that can deliver 10 megabits per second (Mbps) download speed and 1 Mbps upload speed.
[21] 3GPP is the Third Generation Partnership Project. It is an international standards organisation that develops technical specifications for mobile telecoms.
[22] Joint Committee on the National Security Strategy (HC & HL), 2022. *Readiness for Storms ahead? Critical national infrastructure in an age of climate change*. p.8-9

2.25 The Joint Committee on the National Security Strategy has identified that UK telecoms infrastructure is particularly at risk from severe flooding, high winds, and lightning strikes because of climate change.[23]

2.26 Severe weather that results in the loss of mains power or direct physical damage to telecoms infrastructure (such as downed overhead cables) can significantly disrupt or damage telecoms networks.

2.27 As an example, in 2015, BT and Vodafone network nodes in Yorkshire suffered an outage due to severe flooding. This resulted in phone lines to police and hospitals being disrupted, and voice and data services in the North-East were also impacted.[24]

2.28 In 2021, the impact of Storm Arwen left over 74,000 customers without mains electricity supply for over 48 hours.[25] Home broadband routers require power to function, leading to outages for customers until power was restored. Mobile communications were also affected by the storm, as thousands of mobile cell sites were disrupted by the same power outages, affecting all four MNOs.

2.29 As a result of the changing climate, it is increasingly likely that we will see significant telecoms outages during severe storms, potentially threatening human life. Consequently, the resilience and ability of UK networks to maintain services, particularly emergency services, will become more important.

Resilience is being considered across all types of UK Critical National Infrastructure – not just telecoms

2.30 Resilient infrastructure systems are seen by Government as being important, not just for telecoms, but for all CNI sectors. The concept of resilience has been a key element of Government policy since the passing of the Civil Contingencies Act 2004, in which responsibility for the planning, response, and recovery from significant events was transferred in part to local services, businesses, and councils through Local Resilience Forums (LRFs).[26] It has since been adopted into numerous critical areas such as within the National Cyber Strategy and the Integrated Defence Review.

2.31 This focus culminated in the development of the UK Government National Resilience Framework, and all Critical National Infrastructure (CNI) sectors are expected to adopt its core principles.[27] The framework is designed to strengthen the strategic approach that underpins the UK's resilience to all civil contingency risks.

2.32 The UK National Infrastructure Commission's (NIC) 'Anticipate, React and Recover' Report in 2020 presented a new framework for resilience with recommendations for UK Government, regulators and operators of CNI. The NIC report recommends focusing on three main points: setting clear standards of resilience, demonstrating resilience, and continued drive of improved resilience longer term. It recommended that the regulators of the CNI industries should introduce a collection of obligations onto operators to meet government standards of resilience when they are published.

---

[23] Ibid. p.5
[24] Climate Change Committee, 2023. *Progress in adapting to climate change – 2023 Report to Parliament*. p157
[25] Ofcom, 2022. *Connected Nations 2022*. p49-59. Section 4
[26] CO, 2013. *Preparation and Planning for Emergencies: Responsibilities for Responder Agencies and Others*. https://www.gov.uk/guidance/preparation-and-planning-for-emergencies-responsibilities-of-responder-agencies-and-others [accessed 22 November 2023].
[27] HMG, 2022. *The UK Government Resilience Framework*

2.33 On 23 July 2024, the UK Government announced a review of national resilience against the range of risks that the UK faces. [28]

2.34 Examples of resilience measures being undertaken in other UK CNI sectors include National Rail committing £1bn of funding focused on weather resilience to address the increasing challenges and impacts of climate change.[29] Ofwat has announced that it will accelerate potentially £350 million worth of investment in water resilience schemes.[30]

Government has introduced changes to the current framework affecting resilience

2.35 Communications providers have been subject to rules regarding resilience for some time. However, these rules were revised as part of updates to the Communications Act 2003 in 2021, such that PECN/S providers are under a duty to take appropriate and proportionate measures to identify, prepare for and reduce the risk of security compromises, which includes anything that compromises the availability, performance or functionality of the network or service. The legislative framework is summarised in section 3.

Ofcom's own Incident Reporting regime has highlighted where network and service resilience can be improved

2.36 Communications providers are required to inform Ofcom of incidents that have a significant effect on the operation of the network or service. Our procedural guidance for providers explains the types and sizes of incident we expect them to report to us in order for them to comply with their regulatory obligations.[31] These incidents can include outages caused by external factors, such as flooding or power cuts, or internal factors including hardware failure, design flaws or procedural flaws. In 2023, Ofcom received 1,209 reports based on incidents that met the reporting thresholds set out in that guidance. This represented a marginal decrease on the 1,281 reports we received in 2022.

2.37 From the reported incidents, we can track trends in the resilience issues being experienced by providers which provides an indication of how technology changes in the telecoms networks impact networks and services.

2.38 We have been able to identify that over recent years hardware failures were the most common cause of outages, and we can observe the impact of external events such as winter storms on networks. For instance, we saw that winter storms had considerable impact on the number of incidents reported to us between December 2021 and March 2022.[32]

2.39 Where incidents have a particularly significant effect on the operation of the network or service, we engage with providers to establish the cause, how the issue was resolved, and what processes are in place to address how they prevent the issue from reoccurring. In some cases, we have worked with the relevant provider to address our concerns and have seen a reduction in both the number and impact of these events with them.

---

[28] HMG, 2024. *Covid-19 Inquiry Module One: Oral Statement*

[29] Network Rail, 2023. *England & Wales Strategic Business Plan Control Period 7,* p11.

[30] Ofwat, 2023. *Accelerated infrastructure delivery project: final decisions.* p4

[31] Ofcom. *General statement of policy under section 105Y of the Communications Act 2003: Providing procedural guidance on the exercise of Ofcom's functions to ensure compliance with the security duties*

[32] Ofcom, 2022. *Connected Nations 2022*. p.49-59. Section 4

2.40 Incident reporting also enables Ofcom to better understand what is failing in providers' networks, and where in the architecture of the network failures are happening. It allows us to understand what type of failures impact a large number of customers, namely the outages most likely to result in significant harm from loss of service.

Our aim – networks and services we can rely on

2.41 Ofcom's principal duty is to further the interests of citizens in relation to communications matters and the interests of consumers in relevant markets.[33] As part of this, we must also have regard to the desirability of ensuring the security and availability of PECN/PECS.[34]

2.42 Communications providers have a statutory duty to take such measures as are appropriate and proportionate for the purposes of identifying and reducing the risks of security compromises (including Resilience Incidents[35]) occurring. They must also take such measures to prepare for the occurrence of security compromises, again including Resilience Incidents.

2.43 As discussed above, there are a number of ongoing and significant risks to the resilience of the UK's telecoms networks and services. Resilience failures which compromise the availability, performance or functionality of networks and services can have a significantly detrimental impact on consumers. As more people carry out a wider range of day-to-day activities that depend on communications networks and services, the impact of such disruption, on both individual consumers and the wider economy, increases, and ranges from potentially less serious harms (e.g. the inability to access content online for recreational purposes) to much more serious harms (e.g. the inability to communicate during an emergency, or to carry out essential work, or access health or financial services). It is clear therefore that well-functioning communications networks and services are critical both to individual consumers and the wider economy.

2.44 Our aim is to provide guidance which seeks to secure the provision of networks and services which are robust, available and working well, both in the provision of voice calls and the provision of internet access services generally. Communications providers should take measures to ensure provision of services to a generally acceptable level. While we recognise that there will always be situations in which a loss or degradation of service may be unavoidable, disruption to services should be kept to a minimum to avoid unacceptable and unnecessary detriment to citizens and consumers.

2.45 Having engaged with industry, and reviewed current practices and many industry guidelines, we consider that there are a number of measures which providers can and should be taking in order to mitigate the risks of resilience incidents and help ensure the robustness of their networks and services, in accordance with their statutory obligations. Consideration of the measures we have included in our updated guidance should help ensure an appropriate level of resilience for communications services across the UK.

[33] Communications Act 2003 s3(1)
[34] Communications Act 2003 s3(4)(ea)
[35] The Telecommunications (Security) Act 2021 introduces the definition of a "security compromise". The Guidance applies to the sub-category of security compromises relating to the resilience of networks and services, in terms of availability, performance or functionality.

3. The statutory framework

Security duties and guidance under the Communications Act 2003

Summary

3.1 We use this section to outline the statutory framework that underpins the resilience-related security duties imposed on providers of PECN/S. The section also sets out Ofcom's role within this framework.

Security duties and guidance under the Communications Act 2003

3.2 A new security framework for protecting the security and resilience of PECN/S came into force in October 2022. This framework is set out in sections 105A-Z of the Communications Act 2003 (the 2003 Act) and strengthened the existing security duties imposed on PECN/S.

3.3 Section 105A(1) sets out the following general duty: "The provider of a public electronic communications network or a public electronic communications service must take such measures as are appropriate and proportionate for the purposes of— (a) identifying the risks of security compromises occurring; (b) reducing the risks of security compromises occurring; and (c) preparing for the occurrence of security compromises."

3.4 Further general duties are set out in section 105C, which require communications providers to take such measures as are appropriate and proportionate to prevent adverse effects arising from a security compromise that has occurred. Where the security compromise has an adverse effect on the network or service, the provider must take appropriate and proportionate measures to remedy or mitigate that effect.

"Security compromise" includes 'Resilience Incidents'

3.5 The duties imposed by sections 105A and 105C are set by reference to the concept of "security compromise", which is defined in section 105A(2) and includes: "anything that compromises the availability, performance or functionality" of the network or service, and "anything that causes signals conveyed by means of the network or service to be lost".[36]

3.6 "Security compromise" therefore includes both "cyber-type" compromises such as those caused by hackers, and other types of impacts on the resilience of PECN/S, such as outages caused by external factors (e.g., floods, cable cuts, or power cuts) or internal factors (e.g., hardware failure, operational process errors, network design flaws).

3.7 The updated guidance contains measures concerning the sub-category of security compromises relating to the resilience of networks and services, in terms of availability, performance or functionality, or loss of service. As noted above, we refer to security compromises of this nature as "Resilience Incidents".

Relevant Regulations

3.8 In addition to the general duties contained in s105A-D of the Act, the Secretary of State has also made the Electronic Communications (Security Measures) Regulations 2022, which

[36] Communications Act 2003 s105A(2)(a) and (d)

came into force on 1 October 2022 and require communications providers to take specified security measures in accordance with their security duties set out in sections 105A and 105C of the 2003 Act. These Regulations, which also apply in respect of Resilience Incidents, supplement the duties imposed on communications providers by s105A and 105C. They require communications providers to take specified measures including in relation to: network architecture, the protection of data and network functions, protection of certain tools enabling monitoring and analysis, the supply chain, the prevention of unauthorised access or interference, preparing for remediation or recovery, governance, reviews, patches and updates, competency, and testing and assistance.

Guidance given by the Secretary of State in codes of practice

3.9 The Secretary of State also has powers to issue codes of practice under section 105E of the 2003 Act giving guidance to communications providers on the measures to be taken under sections 105A to 105D. In exercise of these powers, the Secretary of State issued the Security Code of Practice setting out guidance for communications providers with relevant turnover in the relevant period of more than or equal to £50m.[37] The Security Code of Practice gives guidance which is mainly related to cyber-type security compromises.

3.10 The updated guidance on resilience is intended to be read in conjunction with the Security Code of Practice, as they both apply to communications providers' networks and services. Where appropriate, we refer to the Security Code of Practice.

Ofcom's Duties and Guidance

3.11 Under the 2003 Act, Ofcom's principal duty is to further the interests of citizens in relation to communications matters and the interests of consumers in relevant markets, where appropriate by promoting competition.[38] In the carrying out of our functions to fulfil this general duty, we are required to secure (among other things) the availability throughout the UK of a wide range of electronic communications services.[39] In the performance of our duties, we must also have regard (among other things) to the desirability of ensuring the security and availability of PECN/S.[40]

3.12 Ofcom must also act in accordance with the six requirements at section 4 of the 2003 Act, of which the following appear particularly relevant: a) the promotion of the interests of all members of the public in the UK, and b) the requirement to take account of the desirability of carrying out our functions in a manner which, as far as practicable, does not favour one form of electronic communications network, electronic communications service or associated facility; or one means of providing or making available such a network, service or facility. [41] We have taken account of these duties in formulating our approach and the Guidance. We have also taken account of our duty to have regard to the desirability of promoting economic growth under section 108 of the Deregulation Act 2015.[42]

3.13 Ofcom has a general duty under section 105M of the 2003 Act to seek to ensure that communications providers comply with their security duties. This gives Ofcom a clear remit

[37] DSIT (formerly part of DCMS), 2022. *Telecommunications Security Code of Practice*
[38] Communications Act 2003 s3(1)
[39] Communications Act 2003 s3()2(b)
[40] Communications Act 2003 s3(4)(ea)
[41] Communications Act 2003 S4(2), 4(5) and 4(6)
[42] The Economic Growth (Regulatory Functions) (Amendment) Order 2024 applies the duty set out in section 108 to Ofcom.

to work with communications providers to improve their security and monitor their compliance.

3.14 In addition, Ofcom is required by section 105Y to prepare and publish a statement of its general policy with respect to the exercise of our functions under sections 105I and 105M-V of the 2003 Act.[43] We published a General Statement of Policy under section 105Y of the 2003 Act in December 2022.[44]

3.15 At the same time, in December 2022, Ofcom also issued guidance on the resilience requirements imposed by, or under, sections 105A to D of the 2003 Act 2003 ("the 2022 Guidance"), in the exercise of our powers under s1(3) and s105Y of the 2003 Act.[45] The 2022 Guidance replaced resilience guidance relating to the previous framework dating from 2017.[46] The 2022 Guidance is superseded by the updated Guidance published alongside this statement and outlined in the next section.

General Conditions of Entitlement

3.16 Communications providers are separately required to comply with the General Conditions of Entitlement,[47] and in particular General Condition A3. This General Condition aims to ensure the fullest possible availability of PECS at all times, including in the event of a disaster or catastrophic network failure. It also requires uninterrupted access to emergency organisations.

3.17 The updated guidance does not give specific guidance on the General Conditions, but it acknowledges those obligations where doing so provides clarity.

[43] Our powers to assess compliance with the security duties (s105N-R) and powers of enforcement of security duties (s105S-V).
[44] Ofcom. *General statement of policy under section 105Y of the Communications Act 2003*
[45] Ofcom, 2022. *Statement: General policy on ensuring compliance with security duties*
[46] Ofcom, 2017. *Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003*.
[47] Ofcom. *General Conditions of Entitlement*.

4. Responses to Ofcom's approach to the Guidance

Summary

4.1 In this section, we explain why Ofcom is updating its resilience guidance, the approach we have taken to this, and how it will be applied. This includes consideration of consultation responses we received on these themes.

4.2 In later sections, we outline the main components of the Guidance, summarise responses and explain the decisions we have taken.

Why we are updating the Guidance

4.3 In December 2023, Ofcom published a consultation: Resilience guidance consultation and Call for Input on mobile RAN power back up ("consultation"),[48] which set out our proposal to update the 2022 Guidance. Alongside this, we also published a draft version of the updated guidance: Network and Service Draft Resilience Guidance for Communications Providers ("proposed guidance").

4.4 When publishing the 2022 Guidance, we explained that we would review and update that version at an appropriate time. We also noted industry had signalled that they would like more guidance on how communications providers can demonstrate compliance with the existing network resilience requirements.

Respondents' view on the scope of the proposed guidance

4.5 Several respondents expressed concerns that the resilience measures included in the proposed guidance risked overlapping with those included within the Security Code of Practice (referred to above at 3.9).[49]

4.6 Fibrus noted concern over the interpretation of "security compromise" as set out in paragraph 3.5 to 3.7 of the consultation. It requested confirmation that reporting requirements will not increase based on resilience incidents, such as outages caused by floods, cable cuts or power cuts, being within scope of security compromises.[50]

4.7 The Federation of Communications Services (FCS) stated that regulation should be focused on the wholesale market.[51]

4.8 Arqiva requested clarification on where the responsibility for providing resilience falls for broadcast services. It further advised that Ofcom should develop a consistent and unified approach outlining the requirements and standards that broadcast licence holders must follow. Additionally, Arqiva emphasised the need for Ofcom to confirm clear roles. This would ensure that, in the event of a major resilience incident, there would be no ambiguity

[48] Ofcom, 2023. *Resilience guidance consultation and Call for Input on mobile RAN power back up*

[49] CityFibre response to the consultation paragraph 19, p4; INCA response to the consultation, paragraph 10, p4; ISPA response to the consultation, p.8; UKCTA response to the consultation, p.5; and Virgin Media O2 response to the consultation, p.22.

[50] Fibrus response to the consultation, p.3.

[51] FCS response to the consultation, p.1.

about responsibility for engaging with affected citizens. Arqiva suggested that clear expectations can then be incorporated into the agreements between the licence holder and the service providers.[52]

4.9 KCOM raised concerns about the proposed position included at 3.2 of the proposed guidance:

"*As explained above, the guidance set out in this document applies to the sub-category of security compromises relating to the resilience of networks and services, in terms of their availability, performance or functionality, which we refer to as Resilience Incidents.*"

KCOM stated "We interpret this in the broadest sense as the ability of an organisation, resource, or structure to be resistant to a range of internal and external threats, to withstand the effects of a partial loss or degradation of platform, system, or service, and to recover and resume service with the minimum reasonable loss of performance." KCOM argued this would be too broad a perspective and might include, for example, systems and processes that support the provisions of PECN/S, but are not, in themselves part of the service, such as financial and IT change systems. It suggested that the introduction of the updated guidance should not result in such systems being subject to scrutiny by the back door.[53]

Ofcom's conclusions and response

4.10 One of Ofcom's regulatory principles is that we will regulate in a transparent manner. Guidance can serve as a useful means of achieving this principle and to increase understanding of Ofcom's policy objectives and approach to regulation.

4.11 We consider that an updated version of the 2022 Guidance is necessary now for several reasons:

a) The Guidance provides greater clarity and detail on how PECN/S can comply with their security duties.
b) Industry has signalled that they would like more guidance on how providers can demonstrate compliance with the existing network resilience requirements.[54]
c) The measures included reflect the changing nature of resilience risks, society's increasing reliance on connectivity, lessons learned from outages beyond the UK, and Ofcom's experience of incident reporting and investigation over the past several years.

4.12 The Security Code of Practice (referred to at above at 3.9) gives guidance on measures which are mainly related to cyber-type security compromises. The technical content of that Code was based on draft guidance developed by experts in the National Cyber Security Centre (NCSC), which was produced following an extensive and detailed analysis of the security of the telecoms sector. The Guidance which is published alongside this Statement relates only to 'Resilience Incidents' and is Ofcom guidance rather than a code of practice made by the Secretary of State made under section 105E of the 2003 Act. We would expect the Guidance to be read in conjunction with the Security Code of Practice, as they both

[52] Arqiva response to the consultation, p.2.
[53] KCOM response to the consultation, p.2.
[54] For example, Ofcom, 2022. *Statement: General policy on ensuring compliance with security duties.* p24. See paragraph 2.90, p.24 (summary of consultation responses). Virgin Media 02 asked for further guidance on how providers can demonstrate compliance as well as practical advice on implementation and compliance, while INCA encouraged Ofcom to engage with all providers on an ongoing basis with regards to the interpretation of the very "high level and general provisions".

apply to providers' networks and services. However, we consider the measures included in the Guidance to be distinct from those included in the Security Code of Practice. While they both relate to 'security compromises', the measures contained in the Security Code of Practice relate primarily to cyber security-related malicious acts or attacks, while the measures in the Guidance relate to distinct aspects of network and service resilience, as defined in section 2.1-2.2 of the Guidance.

4.13 As Ofcom has a duty to ensure that providers comply with their security duties, we consider it helpful to publish guidance that providers can use to understand their resilience-related security duties. Ofcom can also refer to the Guidance when assessing provider compliance or any resilience failures. We are confident that there is no overlap between the measures included in the two documents.

4.14 In respect to Fibrus' query about reporting requirements, our view is that the Guidance is not likely to change existing reporting requirements. Providers are required under section 105K to report security compromises to Ofcom which have a significant effect on the operation of the network or service or put any person in a position to be able to bring about a further security compromise that would have a significant effect on the operation of the network or service. The qualitative criteria and numerical thresholds set out in Ofcom's procedural guidance give our view of which security compromises are likely to be significant and should therefore be reported to Ofcom.[55]

4.15 The Guidance is not expected to impact the existing monitoring programme for the Security Code of Practice. Ofcom will be taking a separate approach to monitoring resilience-related security duties, and we set out our current thinking in the enforcement and monitoring section below at 4.42-4.49.

4.16 In response to FCS, we consider that the Guidance applies to the provision of wholesale network connectivity or services provided to other communications providers or businesses where these are providers of electronic communications services. We state in section 2.2.3 of the Guidance that a publicly available service is one that is available to anyone who is both willing to pay for it, and abides by the applicable terms and conditions, and that the term 'members of the public' requires a broad interpretation; it is not to be read as residential or small business customers. We go on to explain that if a service, such as a virtual private network service, is only likely to attract corporate or commercial customers, is still considered to be available to members of the public if that service is made available to anyone who is both willing to pay for it and to abide by the applicable terms and conditions.

4.17 In response to Arqiva's submission on broadcast services resilience, the security duties which underpin the Guidance are imposed on providers of PECN/S. The main aim of the Guidance is to secure the provision of networks and services which are robust, available and working well, both in the provision of voice calls and the provision of internet access services generally, given these are critical to both individual consumers and the wider economy. However, certain networks and services associated with terrestrial broadcast TV/radio infrastructure comprise PECN/S and consequently fall within the scope of the security duties (as per footnote 24, p18 of the Guidance). The Guidance would therefore

[55] Ofcom. *General statement of policy under section 105Y of the Communications Act 2003.* p.22-35. Section 5, 'Reporting security compromises'.

apply to any such networks, insofar as it is relevant to the provision of these networks and services.

4.18 We do not consider it appropriate to provide additional guidance measures specifically for networks and services associated with terrestrial broadcast TV/radio infrastructure to which the security duties apply. In particular, we note that radio and television services are licensed under the Broadcasting Acts 1990 and 1996, as well as the Wireless Telegraphy Act 2006 and Communications Act 2003. The Broadcasting Act legislation provides a framework under which licensees are obliged to provide a service consistent with the requirements of their Broadcasting Act licences and associated Technical Codes, that together set minimum standards of technical quality, availability and coverage. Many broadcast licensees sub-contract the technical delivery of their services to third-party infrastructure companies. To the extent that these arrangements involved the provision of PECN/S, we consider that those licensees and third parties are best placed to agree technical arrangements and division of responsibility to ensure delivery of the licensed services to the required standards rather than these being specified in Guidance.

4.19 We note KCOM's response, and their view that support systems, such as IT and finance, should not be included within the scope of the Guidance. It would be for providers to consider whether the risk of a network or service resilience type of security compromise occurring is dependent on the running of these systems and take any measures they consider are appropriate and proportionate to reduce those risks. As explained further in this document, any recommended measures included in the Guidance will need to be considered in the context of any given use case, so may not always be necessary or relevant in all scenarios.

Ofcom's approach to preparing the guidance

4.20 We explained in the consultation that Ofcom's approach to preparing the draft guidance had been to consider the established best practice in the telecommunications sector. This approach was informed by:

- examining existing resilience practices at a wide range of providers in the UK and elsewhere; engagement with all of the major fixed and mobile operators, plus a cross section of smaller providers that operate with relatively smaller user bases, e.g., alternative network providers;
- reviewing published standards that have been developed over many years with input from industry; considering any lessons learned from investigations or reviews into resilience-related outages in other comparable countries; and
- referring to evidence collected as part of Ofcom's own incident reporting regime. Close scrutiny of incidents often highlights areas where, in our view, the resilience of networks and services could be improved and where in the architecture of networks failures are happening.

4.21 Based on these factors, the proposed guidance set out a range of high-level good practices in the architecture, design, and operational models that underpin communications networks and services.

Respondents' views on Ofcom's approach to preparing the Guidance

4.22 Several respondents, including BT, BUUK, FCS, Fibrus, Openreach, Vorboss and Voxyonder, broadly supported Ofcom's review of the proposed guidance.[56] IPSA and Vodafone specifically highlighted the flexibility in the design of the guidance so that it could be applied according to provider-specific considerations.[57]

4.23 KCOM noted the proposed guidance contains extensive changes compared to the 2022 Guidance. It raised concerns that updates on this scale within this timeframe could erode trust among providers, as certainty is potentially undermined.[58]

4.24 Several respondents questioned whether Ofcom had undertaken sufficient pre-consultation engagement with a wide enough range of providers. They also queried if the guidance can be applied to a broad mix of different networks.[59]

4.25 INCA argued that the terminology in the consultation is confusing and lacking in definition.[60] It considered the proposed guidance appeared to be based wholly on BT's network and the transposition onto other networks required an improved definition of terms and how they relate to modern network design. It suggested that the proposals cannot be properly assessed until clarity on terminology is provided.

4.26 ISPA and UKCTA highlighted the importance of ensuring that the guidance considers the wide variety of unique network architectures and sizes of network operators within the market. It argued that the current approach risked increasing compliance costs since it would involve adapting to the details of the guidance.[61]

4.27 One provider, [✂] said guidance on minimum skills to architect, develop and implement resilience that is vendor-neutral would be beneficial.[62]

4.28 We received several responses from Scottish public bodies and consumer organisations, which highlighted challenges associated with resilience in rural locations.[63] Scottish Borders Council said it did not believe the proposed guidance sufficiently differentiated areas depending on need and vulnerability, indirectly disadvantaging rural areas as a result. Ofcom's Advisory Committee Scotland (ACS) also said that Ofcom should be cautious in respect of guidance that advises providers to focus on resilience measures based on where the largest number of end users will be at risk, as this will encourage providers to focus on high volume areas exclusively, and to the detriment of remote and rural communities.

4.29 Consumer Scotland and ACS both highlighted concerns that Ofcom's incident reporting thresholds are not sufficient to capture the severity of outages that occur in rural areas. Outages in these areas may affect relatively few consumers compared to densely populated urban areas, and therefore not meet Ofcom's reporting threshold for customers impacted.

---

[56] BT response to the consultation, p.3; BUUK response to the consultation, p.1; FCS response to the consultation, p.1; Fibrus response to the consultation, p.3; Openreach response to the consultation, paragraph 3, p.2; Vorboss response to the consultation, paragraph 2, p.1 Voxyonder response to the consultation, p.1.
[57] ISPA response to the consultation, p.2; Vodafone response to the consultation, p.14.
[58] KCOM response to the consultation, p.1.
[59] CityFibre response to the consultation, paragraph 7, p.2; County Broadband response to the consultation; p.3; ISPA response to the consultation; p.5; Voxyonder response to the consultation, p4.
[60] INCA response to the consultation, paragraph 5, p2.
[61] ISPA response to the consultation; p.6; UKCTA response to the consultation, paragraph 5, p.2.
[62] [✂]response to the consultation, p.3.
[63] Scottish Borders Council response to the consultation, p.1; Consumer Scotland response to the consultation p.5; Ofcom's Advisory Committee for Scotland response to the consultation p.2.

However, their duration may extend into days, representing significant consumer detriment that providers are not obliged to report.

Ofcom's conclusions and response

4.30 We consider that Ofcom's approach to preparing the Guidance is appropriate and proportionate, and that the measures in the Guidance set a baseline for providers to understand what is required of them under sections 105A to D.

4.31 While we note KCOM's view on the need for certainty, we did clearly signal in the 2022 Guidance the possibility of early revisions. The 2017 guidance was updated in 2022 to remove the cyber security related aspects to avoid overlap with the newly created Security Code of Practice. In 2022 we retained the guidance that related to the resilience of networks and services in terms of availability, performance and functionality. We consider the Guidance provides greater detail on resilience measures for providers, as requested by industry responses to our consultation on the 2022 Guidance.[64] This aligns with our commitment to continually improve the clarity and effectiveness of guidance we publish.

4.32 While we note the concerns above regarding the extent of pre-consultation engagement, we consider that we engaged with a reasonable cross section of provider types and sizes to inform the preparation of the proposed guidance. The proposed guidance has now been subject to a public consultation, which has given those providers, not subject to prior engagement, an opportunity to examine the detailed proposals and provide their views and input.

4.33 We acknowledge that a variety of different approaches are taken in network design, and by extension, resilience measures. The Guidance is designed, as far as is practicable, to be technology neutral to reflect this, and to ensure it is future-proofed to ensure that it keeps pace with emerging technologies. However, it would not be practical to publish a single guidance document that accurately encompassed all of the terminology variations used by numerous different network architectures and perspectives of all providers depending on where they sit in the end-to-end network or service value chain. We note that MNOs and several other fixed providers, who responded to the consultation and operate different networks, did not raise concerns that the proposed guidance was too heavily based on BT's network architecture.

4.34 We note concerns raised about aspects of the terminology used in the proposed guidance. As the Guidance is designed to provide a high-level overview of the key network domains that are typical of an end-to-end network or service value chain between end-customer and service/content, Ofcom does not consider it necessary to make significant changes to the terminology used in the Guidance. However, we acknowledge that we can provide additional contextual information explaining that network designs can differ from the general domains included in the Guidance and provide relevant examples where applicable.

4.35 We also highlight that we do not expect all networks to align exactly to a single uniform structure. In that regard, we have removed the optional metro sub-domain from the Guidance as detailed further at 5.11. Where network designs vary, alternative approaches

[64] For example, Ofcom, 2022. *Statement: General policy on ensuring compliance with security duties*. p24. See paragraph 2.90, p24 (summary of consultation responses). Virgin Media 02 asked for further guidance on how providers can demonstrate compliance as well as practical advice on implementation and compliance, while INCA encouraged Ofcom to engage with all providers on an ongoing basis with regards to the interpretation of the very "high level and general provisions".

to resilience may be taken to those set out in the guidance which satisfy the requirements of sections 105A-D. As a result, we have provided additional wording in section 1.3 of the Guidance to reflect these points.

4.36 We recognise the difficulties in assessing the impact and duration of some outages in rural areas, and the subsequent impact on customers who rely on them, particularly when other connectivity options are limited. As outlined later in section 8, we plan to do further work to understand where and when further power back up may be required. This may result in further changes in future.

4.37 We plan to propose changes to our procedural guidance, and part of our work will include consideration of updating Ofcom's incident reporting thresholds. As part of this, we will be looking at the options that are potentially available to better capture the occurrence of telecoms outages in rural areas.

4.38 We also acknowledge that we could provide additional qualification to the Guidance in relation to the factors that providers should consider when deciding on the appropriate and proportionate resilience measures for single points of failure, to avoid the interpretation that we would only expect measures to be in place in densely populated locations. We have updated the Guidance in 4.4.1 to highlight that providers should consider the geographical size of the coverage area impacted by a given failure as a factor when determining where to prioritise resilience measures, in recognition that outages in rural areas may have a widespread impact that affects entire communities. This reference is consistent with point 5.40 in our 2022 Guidance.

Enforcement and monitoring

4.39 Several providers suggested the proposed guidance was too prescriptive and should be more outcomes based. They also queried whether providers had any discretion when following the measures.[65]

4.40 Some respondents requested clarification about Ofcom's approach to monitoring compliance with providers' resilience-related security duties.

Ofcom's conclusions and response

4.41 We note concerns that the proposed guidance is too prescriptive, however, we consider the level of detail appropriate, with the measures included in the guidance representing established good practice, based on the factors we set out above at 4.21.

4.42 We also consider those measures are appropriate and can help providers to comply with their resilience-related security duties. We have not set out specific measures in relation to every possible use case, which would in our view be impractical. As we stated in the consultation, Ofcom has been mindful to avoid being overly prescriptive on how networks should be designed in every specific aspect.

4.43 We also note queries on whether providers have any discretion in applying the Guidance. It is for providers to assess for themselves (taking this Guidance into account) which measures are appropriate and proportionate in their own particular cases. For example, large

[65] ISPA response to the consultation, p.7; Virgin Media O2 response to the consultation, p3; UKCTA response to the consultation, paragraph 4, p.2.

providers with significant numbers of users may require a more comprehensive set of measures compared to those with smaller customer bases.

4.44 The Guidance is intended to set out the general approach which we would normally expect to take in investigating compliance with s105A-D as appropriate. It is not the only way for providers to comply with their resilience-related security duties under s105A-D and is not binding. A provider may choose to comply with their resilience-related security duties by adopting different technical solutions or approaches to those specified in the updated guidance. Where a provider has taken a different approach to that set out in the Guidance, we would expect them to be able to explain what approach they are adopting to meet their resilience-related security duties.

4.45 As with the 2022 Guidance, we intend to use the Guidance as a practical reference both:

- in continuing to build on our understanding through engagement with providers and wider industry, and monitoring the resilience of networks and services; and
- as a starting point for considering compliance as part of any enforcement activities in relation to resilience issues.

4.46 While the publication of updated guidance is intended to improve transparency and understanding of Ofcom's expectations around the relevant resilience-related security duties, our view is that providers should already be taking measures in order to comply with their resilience-related security duties.

4.47 We will consider any compliance issues having regard to the circumstances at the time. As set out in Ofcom's enforcement guidelines, we make decisions about whether to open investigations on a case-by-case basis, having regard to our statutory duties and all the matters that appear to us to be relevant. In doing so, we exercise our discretion to target action at cases we think are most likely to produce good outcomes for citizens and consumers.[66]

4.48 The Ofcom procedural guidance explains how we will use our powers under the revised security framework, both in the context of compliance monitoring and enforcement. Our powers include:

a) information gathering powers under section 135 of the 2003 Act – see sub-section titled "Information-gathering powers (section 135)" in section 3 of the Ofcom procedural guidance.
b) assessment powers under sections 105N and 105O of the 2003 Act – see subsection titled "Powers to assess compliance – Assessments and assessment notices (sections 105N105Q)" and sub-section titled "Powers to assess compliance – Power to enter premises (section 105O and 105R)" in section 3 of the Ofcom procedural guidance.
c) enforcement powers under sections 105S to 105V of the 2003 Act – see section 6 of the Ofcom procedural guidance.

[66] Ofcom, 2022. *Regulatory Enforcement Guidelines for investigations, Guidelines*.

Impact Assessment

4.49 Several respondents questioned why Ofcom had not conducted a fully costed impact assessment.[67]

4.50 Section 7 of the 2003 Act requires us to carry out and publish an assessment of the likely impact of implementing a proposal which would be likely to have a significant impact on businesses or the general public, or when there is a major change in Ofcom's activities. More generally, impact assessments form part of good policymaking and we therefore expect to carry them out in relation to a large majority of our proposals.

4.51 We use impact assessments to help us to understand and assess the potential impact of our policy decisions before we make them. They also help us explain the policy decisions we have decided to take and why we consider those decisions best fulfil our applicable duties and objectives in the least intrusive way. Our impact assessment guidance sets out our general approach to how we assess and present the impact of our proposed decisions.

4.52 The relevant duties in relation to the Guidance are set out in Section 3 (the legal framework). The analysis presented in our consultation document constituted an impact assessment as defined in section 7 of the 2003 Act. We assessed the proposed guidance against the alternative, the retention of the 2022 Guidance which would remain in place but provides significantly less detail. The proposed guidance set out those changes which we considered would most effectively and proportionately satisfy our objectives compared to that counterfactual.

4.53 We note comments made about the nature of the impact assessment included in the consultation. For each of the sets of measures we set out (physical planes, control planes etc.), we explicitly considered whether the proposed measures would produce adverse effects which are disproportionate to the aim pursued. Our approach was qualitative rather than quantitative. Given the wide scope for differences in the nature and scale of potential measures that can be taken, it is questionable if any range of numbers produced would be useful to inform a discussion on proportionality in this instance.

4.54 Our consideration of stakeholders' responses concerning the impact of the Guidance is contained throughout this section and sections 5, 6 and 7 of this document. This includes the impact of implementing the measures included in the Guidance (insofar as they are not already implemented by providers) at the physical network infrastructure domains (5.131-5.150), the control plane (6.36-6.58), the management plane (6.82-6.98), communications providers' own services (6.139-6.146), and processes, tools, and training (7.47-7.71).

4.55 We also consider that providers will benefit from the Guidance as they will have further clarity on how we expect them to meet their resilience-related security duties.

4.56 We expect use of the Guidance to result in an overall positive impact for consumers, citizens and business by ensuring more reliable communications and internet services that meet the needs of increased societal demand for them.

[67] INCA response to the consultation, p.6; ISPA response to the consultation, p.7; KCOM response to the consultation, p.3; Virgin Media O2 response to the consultation, p.4.

Impact on Communications Providers

4.57 The Guidance aims to provide additional clarity for providers regarding their duties imposed by and under s105A-D and seeks to reflect the changing nature of resilience risks and is future proofed to the greatest extent possible.

4.58 Whilst we recognise that there may be some additional costs associated with providers amending their network infrastructure approaches in order to implement the measures set out in our Guidance, we consider that the benefits outweigh any potential costs. For example, we expect that, when providers are interconnecting their voice services with other providers, this should avoid the wider internet. We explain that there are measures providers can take to interconnect voice services in a resilient way but that this may incur some costs. We go on to explain that we consider the benefits of these resilience approaches, such as avoiding risks to end users' ability to make critical calls, significantly exceed these costs. Measures contained in the Guidance are flexible enough to apply to all types of provider offering communications networks and services in the UK, while also allowing for continued technology evolution, and providers may choose to comply with their resilience-related security duties by adopting different technical solutions or approaches to those specified.

4.59 We also expect that this flexibility and the technology and network agnostic positioning of our measures (4.34) will limit the impact of the Guidance on competition. In addition, we consider the use of the customer hours lost metric helps to ensure that smaller providers are not disproportionality impacted by certain measures in the Guidance.

Impact on citizens, consumers, and businesses

4.60 The Guidance aims to improve the resilience of providers in a way that benefits citizens and consumers. Any additional costs that might be passed on to them are likely to be outweighed by the benefits to citizens and consumers that comes from a reduction in service outages and customer hours lost, and improved service quality.

Equality impact assessment

4.61 Section 149 of the Equality Act 2010 (the "2010 Act") imposes a duty on Ofcom, when carrying out its functions, to have due regard to the need to eliminate discrimination, harassment, victimisation and other prohibited conduct related to the following protected characteristics: age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex and sexual orientation. The 2010 Act also requires Ofcom to have due regard to the need to advance equality of opportunity and foster good relations between persons who share specified protected characteristics and persons who do not. Section 75 of the Northern Ireland Act 1998 (the "1998 Act") also imposes a duty on Ofcom, when carrying out its functions relating to Northern Ireland, to have due regard to the need to promote equality of opportunity and have regard to the desirability of promoting good relations across a range of categories outlined in the 1998 Act. Ofcom's Revised Northern Ireland Equality Scheme explains how we comply with our statutory duties under the 1998 Act.

4.62 To help us comply with our duties under the 2010 Act and the 1998 Act, we assess the impact of our proposals on persons sharing protected characteristics and in particular whether they may discriminate against such persons or impact on equality of opportunity or good relations. In particular, section 3(4) of the Communications Act 2003 also requires

us to have regard to the needs and interests of specific groups of persons when performing our duties, as appear to us to be relevant in the circumstances. These include:

a) the vulnerability of children and of others whose circumstances appear to us to put them in need of special protection;

b) the needs of persons with disabilities, older persons and persons on low incomes; and

c) the different interests of persons in the different parts of the UK, of the different ethnic communities within the UK and of persons living in rural and in urban areas.

4.63 We do not consider that the publication of the Guidance will affect any specific groups of persons (including persons that share protected characteristics under the 2010 Act or the 1998 Act) differently to the general population. This is because the Guidance relates to the measures to be taken by all providers of PECN/S, so all customers who use these services should see an overall benefit from their implementation, irrespective of their protected characteristics, and the part of the UK in which they live. We have taken into account the needs of those who live in more rural locations, when for example, we have included provisions that when considering network architecture, design, and operational models, we expect providers to put in place measures which specifically consider a number of factors, including the geographic distribution of equipment, as well as the number of customers impacted during different types of failures. This should help to ensure that the needs of rural communities are considered in the implementation of resilience measures by providers.

Welsh language

4.64 The Welsh Language (Wales) Measure 2011 established a legal framework to impose duties on certain organisations to comply with 'Standards' in relation to the Welsh language. In January 2017, the Welsh Language Commissioner issued a compliance notice to Ofcom. This lists 141 Standards which Ofcom must meet when carrying out its work to ensure that it treats Welsh no less favourably than English.

4.65 Where the Welsh Language Standards are engaged, we consider the potential impact of a policy proposal on: (i) opportunities for persons to use the Welsh language; and (ii) treating the Welsh language no less favourably than the English language. We also consider how a proposal could be formulated so as to have, or increase, a positive impact, or not to have adverse effects or to decrease any adverse effects.

4.66 We have considered these matters. We are not aware, despite consulting publicly on a set of resilience proposals, of evidence suggesting that there would be any obvious issues resulting from the issuance of the guidance that directly relate to the Welsh language. Further, our guidance measures are focussed principally to help providers better understand their resilience-related security duties imposed by and under sections 105A-D and to help achieve the overall objectives which are to identify, respond to, and prepare for the occurrence of security compromises – and specifically resilience incidents. Our guidance measures do not focus on matters that would directly result in the sharing of information with citizens or consumers.

5. Resilience guidance for physical infrastructure domains

Summary

5.1 In this section, we present our analysis and conclusions on the key measures that will be included in the Guidance related to the physical infrastructure domains. The Guidance should help providers better understand and meet their existing resilience duties under section 105A to D.[68]

5.2 In summary, we have concluded that most of the measures outlined in the proposed guidance will be retained in the final version. However, we have made some revisions to the proposals, based on responses to the consultation, including those relating to power backup at fixed cabinets.

5.3 We set out the measures included in the proposed guidance, summarise respondents' views on them and explain why we consider the final set of measures included are appropriate and proportionate.

Network infrastructure domains

5.4 This section considers responses to the consultation's question regarding the appropriateness and proportionality of the resilience proposals at the various infrastructure domains.

5.5 The proposed guidance stated that the network infrastructure within a provider's network (see figure 3 in the proposed guidance) can usually be broken down into the following domains:

- Access / Last Mile;
- Aggregation / Backhaul;
- Core / Metro; and
- Peering and Interconnect.

Consultation proposal for measures at the Access / Last mile domain

5.6 We explained that access networks provide network connectivity to the end-customer site or device. The proposed guidance explained that the access domain, both fixed and mobile, is often associated with having certain features that can present specific types of resilience

[68] The final set of Guidance is in Annex 1.

challenges. In particular, access domain infrastructure tends to be much more extensive and geographically dispersed than other domains, and therefore subject to significantly more single points of failure. It would also be quite costly to ensure significant amounts of resilience at all access nodes. To give some sense of scale, the access domain currently supports approximately 28 million fixed line broadband connections throughout the UK.

5.7 The proposed guidance (section 4.2.1) set out measures that we expect providers to take to mitigate against resilience challenges at the access domain. These were mostly concerned with providers ensuring that access networks are designed to avoid or reduce the single points of failure. For example, when considering network architecture, design, and operational models, we stated an expectation for providers to put in place measures which specifically consider a number of factors, including the geographic distribution of equipment as well as the number of customers impacted during different types of failures.

5.8 We noted that access network equipment, or locations such as mobile base stations and street cabinets, are often connected to a single 'parent' site without resilient connectivity. In cases where greater resilience is appropriate and proportionate, we explained in the consultation that providers should provide cabinets (fixed) or mobile base stations with a connection to an additional parent site.

5.9 Further, in the consultation, we explained that we would expect network equipment within access sites to have automatic failover functionality built in, so that when equipment fails, network traffic is immediately diverted to another device or path that can maintain end user connectivity.

5.10 We also covered the issue of power back up for equipment in the access domain. However, we will consider that measure when examining the power back up measures in the Core domain at paragraph 5.89 below.

Summary of responses to the proposed measures at the Access / Last mile domain

Dual parenting and automatic failover measures

5.11 Several respondents commented on the use of resilient connectivity (or 'dual parenting') in the access/last mile domain.

5.12 One provider, [✂] welcomed the flexibility of the proposed approach, e.g., take measures only in cases 'where greater resilience is appropriate'. However, it also had concerns about the projected level of costs if it was expected to implement 'dual fed' connections in all access level scenarios.[69]

5.13 Three sought clarification on "the scenarios where greater resilience is to be considered appropriate" and pointed out "that having dual links from mobile base stations to two parent sites is cost prohibitive."[70]

5.14 Virgin Media 02 said it would "welcome clear guidance on what factors can be taken into account when determining what is 'appropriate' when equipping resilience connectivity to an additional parent site. Further, that it does not believe that the proposed guidance or

[69] [✂] consultation response, p.5.
[70] Three consultation response, p.4.

Impact Assessment properly recognises the difficulty and cost of adding resilience in the last mile.[71]

5.15 Several respondents provided comments on the proposed automatic failover measures, specifically within the access domain.

5.16 Azenby Ltd. stated that "automatic fail-over of individual sites (to an alternative parent site/route) mentioned in paragraph 4.26 of the consultation would not be practical in the case of mobile network base stations."[72]

5.17 Openreach argued that implementing automatic failover at this level would not be proportionate due to the relatively small number of customers affected in each particular access network and the associated costs.[73] Openreach also commented more broadly that "the text tends to imply that the base level assumption is that providers are expected to architect FTTC based networks to meet a much higher default level of resilience than is currently viable."[74]

5.18 Virgin Media O2 highlighted a disparity between the proposed guidance and consultation text on how automatic failover should be implemented. It requested further clarification on this apparent mismatch.[75]

5.19 Virgin Media O2 also said the proposed guidance on automatic failover, which sets an expectation that "equipment within the access sites supports mechanisms to automatically fail over between core sites, and services should be maintained or re-established automatically", should acknowledge that there may be exceptions, particularly for older technologies. It noted the challenge of applying this to 2G and 3G base stations and base station controllers.[76]

5.20 [✂] requested clarification on this sentence: "For 3GPP-mobile-based networks, over-reliance on a single source (or path) of network timing/synchronization is a weakness", in relation to how a dual-timing/synchronization architecture is implemented. [77]

Ofcom assessment of responses to the proposed measures at the Access / Last mile domain

Dual parenting and automatic failover measures

5.21 While our overall approach to dual parenting and automatic failover measures in the Guidance broadly maintains the approach taken in the consultation, consultation responses highlighted that our proposed guidance was not sufficiently clear in certain respects.

5.22 The proposed guidance explained that, *in cases where greater resilience is appropriate*, an access site (mobile base station or fixed cabinet) should be connected to an additional parent site. However, following our review of responses, we appreciate that the wording used to describe that particular measure may have been misunderstood or may not apply usefully to all network architectures. Further, the original form of words in the consultation

[71] Virgin Media 02 consultation response, p.19.
[72] Azenby Ltd. consultation response, p.2.
[73] Openreach consultation response, p.4.
[74] Openreach consultation response, p.4.
[75] Virgin Media 02 consultation response, p.18.
[76] Virgin Media 02 consultation response, p.17.
[77] [✂] consultation response, p2.

document (i.e. '*providers should provide cabinets (fixed) or mobile base stations with a connection to an additional parent site'*) may have created an impression that we were proposing a more onerous set of measures than we had intended in the access/last-mile domain, and this prompted concerns about the proportionality of the proposals.

5.23 We did not intend for the text to imply that every fixed access cabinet or base station should have dual connectivity back into the network. We recognise this would not have been proportionate, given the likely costs involved. There were two key principles that were intended.

5.24 The first principle was that an access network site should be designed and configured to survive the loss of a core site, and automatically fail over between core sites (based on our definition of a 'core' site). This assumes that there is an aggregation/backhaul network domain in between the access and core network domains which has the relevant resilient connectivity to core sites needed in order for the automatic failover between core sites to be possible.

5.25 The second principle is related to connectivity resilience 'where appropriate' from the access network site to the aggregation/backhaul network, or towards the core more generally. It would be for the provider to determine how much resilience is appropriate depending on factors known only to the provider in question.

5.26 However, our reading of some responses suggests our intentions here were not sufficiently clear. The notion of connectivity from an access site to an additional parent site 'where appropriate' was intended to be only one of a broader set of potential connectivity options towards the core; noting that some networks may make use of more than one aggregation/backhaul network technology or provider. Our view is that in practice, each scenario will be different, and the provider needs to base their architecture/design decisions on the circumstances of any given case. We have revised the drafting of the final guidance to make these points clearer.

5.27 We note Virgin Media O2's comments about automatic failover related to challenges of 2G and 3G base stations and base station controllers (BSCs & RNCs). We highlight that these are RAN functions, and that in most traditional mobile networks, BSCs and RNCs were often deployed in regional 'aggregation sites' rather than 'core sites'; although this may have changed over time as 3G and 2G network components have been replaced in order to support higher capacities and IP transport interfaces. In any case, we accept that some 2G and 3G RAN components may not support the type of resilience mechanisms that we expect of 4G and 5G networks. As 3G and 2G networks are being switched off, and usage is minimised, we see this as a diminishing issue. We are content to note this challenge in the Guidance but continue to encourage the capability to be used in 2G/3G RAN components that support it.

5.28 In response to [✂] comment about 3GPP mobile networks, we are not proposing specific implementations of resilient timing architectures because appropriate solutions may vary based on the nature of the specific RAN deployment model. As such, each provider should assess the risks of their RAN and backhaul connectivity model and technologies in relation to timing/synchronisation reliability and the impact that this could have on the overall RAN deployment. They should then make appropriate design decisions based on the risks and potential impacts.

Changes included in the Guidance at the Access / Last mile domain resulting from the consultation

5.29 Following on from the above, we have added some further detail to the final guidance to help providers determine what factors should be considered when judging what is an appropriate level of resilience at any given site. These factors include but are not limited to:

a) the number of customers that would be impacted by a given failure;
b) the service level requirements and criticality of the services being provided; and
c) whether the degree of connectivity resilience is appropriate for the customers being served by that site.

We seek to ensure these factors remain flexible and are not overly prescriptive to allow providers to determine measures that are appropriate and proportionate to their own circumstances.

5.30 We recognise the point made by several respondents that the measures relating to automatic failover appear to have been described differently in the consultation document compared to the proposed guidance document. We appreciate the wording in the former may have left the impression of a much more onerous set of measures than we had intended. We consider that the wording in the proposed guidance document is a more accurate description of our intention than the wording in the consultation document.

5.31 To clarify, our expectation is that automatic failover functionality should be implemented to support failover between core sites as indicated above in paragraph 5.9. We consider this approach better reflects our expectation of the relationship between access networks in the automatic failover of core sites. We also consider making these clarifications helps ensure that these measures are appropriate and proportionate.

5.32 We have also made a small change to the introduction section of the proposed guidance following a point made by BT about a reference to the Centre for the Protection of National Infrastructure (CPNI) guidance.[78] CPNI has been replaced by the National Protective Security Authority (NPSA).[79] We agree it is appropriate to make reference to the NPSA guidance in addition to the Security Code of Practice.

Consultation proposal for active cabinets at the fixed access level domain

5.33 A further key risk at the access network level, set out in the proposed guidance, is the potential for loss of electrical power for active equipment in cabinets and walk-in cabins in fixed networks ('active cabinets'). We explained a range of technology deployment models that can be used to provide broadband connectivity to customers' premises. Some technologies use street level infrastructure, such as cabinets, to ensure connectivity between the provider and the customer. Some cabinets rely on electrical power from the power distribution grid and cannot function without it. These 'active cabinets' are at risk from localised power outages, which could result in customers losing connectivity until power is restored.

[78] BT response to the consultation p.14.
[79] https://www.gov.uk/government/organisations/centre-for-the-protection-of-national-infrastructure

5.34 We considered that providers should maintain a normal level of service in the event of a local power outage. We proposed therefore that, where providers have active cabinets in place, they should have adequate power backup to ensure they maintain services for a minimum of 4 hours in the event of a power outage at those cabinets. The proposed guidance set the expectation that the backup measures would not apply to active cabinets being removed from the network within 5 years.

Summary of responses for active cabinets at the access level domain

Responses on costs

5.35 Some respondents explained that some providers do not currently provide a minimum of 4 hours back up, and raised concerns about the costs that would be incurred to implement this measure. INCA and [✂] expressed concern regarding the cost burden of implementing a higher standard of battery backup after their networks have already been built. They argued that the level of costs could threaten the continued operation of some providers.[80]

5.36 Virgin Media O2 argued that the cost and complexity (and time it would take) to retrofit existing networks is far more significant than Ofcom has assumed. Further, that it did not believe it is appropriate or proportionate to mandate that all existing cabinets are retrofitted to provide a minimum of 4-hour battery backup, but if some requirement to retrofit existing networks is retained in guidance, then cabinets which are expected to cease serving customers within the next 10 years ought to be excluded.[81] It also argued that the timeframe in which providers would be expected to plan and implement these measures would affect feasibility and costs.[82]

5.37 Virgin Media O2 and [✂] argued Ofcom did not collect information in relation to the extent of existing fixed street cabinet power backup, or cost initial estimates of implementing these measures which are significant.[83]

5.38 Some respondents highlighted the risks of decline in battery performance over the longer term or in certain conditions, and its impact on meeting the 4-hour requirement. INCA, UKCTA and Virgin Media O2 argued that battery life is affected by temperature and use, and a battery will deteriorate over time and, at some point, will need to be replaced.[84]

5.39 Openreach argued that, although it proactively deploys built-in battery back up to cabinets, actual performance will be affected by the age of the battery, the state of the battery charge when the outage occurs, and the real-time load on the battery during the power failure. Further, that the 4-hour minimum proposal would require them to re-engineer their access network to meet the higher default level of resilience and could result in major diversions of resources and potentially high levels of stranded costs.[85]

5.40 Some respondents chose to highlight the ongoing operational costs associated with implementing the power backup proposal. INCA and [✂] raised concerns regarding the

[80] INCA response to the consultation, paragraph 17, [✂]response to the consultation, p.5.
[81] Virgin Media O2 response to the consultation, p. 13.
[82] Virgin Media O2 response to the consultation, p. 15.
[83] Virgin Media O2 response to the consultation, p. 14 , and [✂]response to the consultation.
[84] INCA response to the consultation, paragraph 20, p.4; UKCTA response to the consultation, paragraph 11, p.3; Virgin Media O2 response to the consultation, p.14.
[85] Openreach response to the consultation, paragraphs 16-19, p.4.

whole-life costs associated with power back up. These costs include ongoing maintenance, such as the replacement of battery packs, and the implementation of recurring monitoring systems to assess remaining battery capacity. They questioned whether these additional expenses are sustainable within the current budgets.[86]

5.41 Some providers highlighted the additional risks to active cabinets of installing battery backup measures – notably fire risk and additional risk of theft.[87]

5.42 Some providers argued that the provision in the proposed guidance that exempted those active cabinets that were due for decommission, or replacement, within the next 5 years would have minimal effect. Virgin Media O2 and Openreach argued that despite the roll out of new full fibre lines, it was not necessarily the case that all customers would be migrated to the new infrastructure so quickly, and these active cabinets could still be in use beyond the current decade.[88]

5.43 Some respondents urged further consideration of the impact of additional battery use on the environment. For example, the increased presence of lead and acid batteries, waste disposal etc should be relevant to considering what is appropriate and proportionate.[89]

5.44 Sky argued that the resilience guidance should not limit providers from entering into agreements to gain access services from third party wholesale providers that do not meet Ofcom's power resilience criteria. Instead, it proposed ensuring power resilient new build or retrofitting over time in the access supply chain as a more proportionate solution.[90]

Responses on the benefits of back up

5.45 Aberdeenshire Council argued that a minimum of 4 hours power resilience in the event of power outages is simply not enough for some areas, in some situations. It explained that Storm Arwen saw power outages over several days for many properties in Aberdeenshire. It added that the new guidance should look to extend the 4-hour requirement, particularly for locations that have previously suffered from extended power outages (i.e. periods of 48 hours or more). [91]

5.46 SynOptika Ltd did not agree that 4 hours back was long enough. It argued that long duration power outages will become more common due to climate change and that networks need to consider resilience, by design.[92]

5.47 Azenby Ltd. argued that, rather than a fixed 4-hour standby for all street cabinets, the guidance could specify a graduated range, for example, 2-6 hours depending on the number and capacity of dependent end-user equipment.

5.48 Some respondents argued that there may be limited benefit from imposing a minimum backup requirement of 4 hours. INCA and [✂] argued that this requirement would not be appropriate or proportionate given the limited benefit to customers. For instance, a provider might supply connectivity, during a mains outage, up to the boundary of the

[86] INCA response to the consultation, paragraph 19, p.4; [✂] response to the consultation, p.5.
[87] UKCTA response to the consultation, paragraph 11, p.3; Virgin Media O2 response to the consultation, p.15
[88] Openreach response to the consultation, paragraph 19 p.5; Virgin Media O2 response to the consultation, p.13.
[89] ISPA response to the consultation, p.5; UKCTA response to the consultation, paragraph 10; Virgin Media O2 response to the consultation, p.15.
[90] Sky response to the consultation, p.4.
[91] Aberdeenshire Council response to the consultation, p.2.
[92] SynOptika Ltd response to the consultation, p.2.

customer's property, but the customer may lack power backup in their premises for voice/ router devices. Consequently, in a power outage, connectivity could still be disrupted.[93]

5.49 Virgin Media O2 made the same point but also argued their current fixed network is more likely than other networks to experience power outages at street cabinets and at home simultaneously. It explained that their DOCSIS / HFC cabinets are more numerous and geographically closer to the customer than an OLT on a full fibre network. [94]

Responses on who should be responsible for power outages

5.50 Virgin Media O2 argued that electrical power backup for active cabinets should be considered holistically as part of a wider cross sector consultation on power resilience before implementing in guidance, similar to Ofcom's Call for Input on mobile RAN backup.

5.51 Some respondents argued that responsibility for power resilience should not fall solely on the telecoms sector. County Broadband, INCA, UKCTA and Virgin Media O2 argued that the primary responsibility to improve resilience of the power supply should sit with electricity Distribution Network Operators (DNOs)[95]. INCA and [✂]argued that a balanced approach needs to be adopted, which distributes the responsibility with regard to resilience of power supply reasonably between telecoms operators and power companies.[96]

5.52 Some respondents argued that more could be done to ensure that electricity service restoration to providers' network infrastructure is prioritised in the event of an unplanned power outage. CityFibre, CCUK, INCA, ISPA, UKCTA; Virgin Media O2; and Vorboss argued electricity DNOs should ensure greater prioritisation of energy supply to providers' sites and to consumers.[97] In particular, CityFibre argued more could be done to build on the work undertaken by the EC-RRG in 2022 to plan for power supply interruption scenarios.[98] [99]

5.53 The Joint Radio Company questioned whether the costs associated with an intervention limited to enhancing commercial communications network operational performance might be better addressed through alternative strategies, such as enabling spectrum access to the Energy Network Operators to deliver enhanced operational control capability.[100]

Assessment of responses to proposal for active cabinets at fixed access level

5.54 We remain concerned about the nature and scale of harms that might result from local power outages impacting active cabinets. Losing connectivity can cause significant harm to individuals, including that caused by a loss of ability to make emergency calls. We therefore consider it important for providers to consider what can be done to maintain services during a power outage to help avoid these harms and that the Guidance should reflect this.

---

[93] [✂] response to the consultation, p.7; INCA response to the consultation, paragraph 29, p.6.
[94] Virgin Media O2 response to the consultation, p. 16.
[95] County Broadband response to the consultation, p.2; ISPA response to the consultation; p.4; UKCTA response to the consultation, paragraph 8, p.3; Virgin Media O2 response to the consultation, p. 10.
[96] [✂] response to the consultation, p.4; INCA response to the consultation, paragraph 27, p.6.
[97] CCUK response to the consultation, paragraph 11, p.2; INCA response to the consultation, paragraph 30, p.6; ISPA response to the consultation, p.4; UKCTA response to the consultation, paragraph 9, p.3; Virgin Media O2 response to the consultation, p. 10; Vorboss response to the consultation, p.2.
[98] CityFibre response to the consultation, paragraph 13, p.5.
[99] EC-RRG, 2022: *2021/2022 Severe Storms Post-Incident Report*.
[100] Joint Radio Company response to the consultation, p.1.

We must also ensure that any expectations we set in the Guidance are appropriate and proportionate.

5.55 While we continue to consider that the Guidance should set expectations on an appropriate level of power backup, the information provided in responses to the consultation has led us to consider that the nature and scale of costs needed to retrospectively upgrade active street cabinets to meet the specific requirements of the proposal may be greater than was initially anticipated. While a minimum of 4-hour battery backup may be a typical practice for many providers when installing *new* active cabinets, the consultation has revealed that:

a) it may not have necessarily been typical practice to include backup in installations in the past, and even those that have installed backup cannot necessarily provide 4 hours' worth of back up in all cases;
b) batteries that have been in place for a while, on existing networks, may not perform in a way that can provide enough power to maintain service for 4 hours or more (due to degradation over time and exposure to other external factors such as cold weather);
c) Some existing networks use cabinets that, at present, cannot house additional batteries that would perform for 4 hours, and would likely require entirely new and larger cabinets to be rolled out to meet the proposal.

5.56 Assessing the capability of *existing* networks to meet the proposed 4-hour minimum requirement may be challenging and may vary significantly between providers. This uncertainty extends to the potential cost implications for providers of retrospectively upgrading their active cabinets to achieve this specific target. Based on the evidence now available, we cannot be confident that including such a specific measure, a minimum 4-hour backup power supply that extends to all *existing* powered active components in street cabinets, would be a proportionate measure within the guidance. We therefore, set out below how we have addressed this issue in the Guidance.

5.57 In response to the Joint Radio Company's point, in June 2023, Ofcom published a Call for Input on five potential candidate spectrum bands that might be suitable to support the future operational communications needs of the utilities sector. Our work in this area supports government's work to ensure a system that is fit for the future needs of the smart grid – it is currently looking at the cost of all options to ensure value for money for energy consumers. In November 2023, Ofcom stated that it will provide a further update on our next steps in due course, including any plans to consult on specific proposals should access to new spectrum be required to support a private network, and that we are continuing work to confirm the suitability of these bands for use by the utilities sector.

5.58 We note Sky's request that the guidance should not prevent providers from entering into agreements with third party access providers. We do not consider that the guidance, by itself, would prevent providers from entering into commercial agreements with one another. It would be for providers themselves to consider whether the resilience-related security duties apply to them and take any actions they consider necessary to comply with those duties.

Changes included in the Guidance for active cabinets at fixed access level resulting from the consultation

5.59 In light of feedback from the consultation, we have decided to revise the expectations set out in the proposed guidance so that they only apply to active cabinets that are yet to be installed. We are confident about including an expectation that applies to active cabinets

which are planned to be installed, as costs for sufficient mains electricity backup, including batteries, can be included in the design and build costs. Cabinets with adequate capacity to house batteries can be specified early, and power backup installation costs can be much more easily absorbed by the initial build costs.

5.60 At this stage, we will not specify a *minimum* backup duration time for planned active street cabinets. In the consultation, we explained that a minimum of 4 hours back up would be appropriate as our understanding, from engagement with a selection of fixed-access providers of various sizes, was that this was typical practice. However, given the information presented in the responses, particularly that 4 hours cannot always be achieved due to deterioration and other factors, we will not specify a minimum time at this stage. Instead, we explain that providers should consider several factors when determining the extent of power back-up to provide in street cabinets, including:

a) Observed duration of outages: Providers should consider sufficient power backup that will likely cover expected duration of outages. Ofgem national power outage, averaged over the last four years, suggests that around 93% of power outages experienced by customers are less than 4 hours, while around 90% are less than 3 hours, which should serve as a general guideline for the expected duration of outages (some areas, particularly in rural parts of the country, may experience mains power outages that are longer than the national average);[101]
b) Energy supply risks to industry: If government was to initiate the Electricity Supply Emergency Code (ESEC), which uses a Variable Rota Disconnection Plan, then mains power disconnections would have a nominal disconnection period of 3 hours, but there may be delays of restoration of some load blocks by up to an hour. Therefore, power could be out for approximately 4 hours in a given rota disconnection window for a given ESEC level;[102]
c) Relative cost: Depending on the location of a cabinet, the number of customers served, and other factors, the additional cost of providing power backup could vary significantly. Where the incremental cost is relatively high, we would only expect it to be proportionate to provide additional power backup if the number of customers potentially impacted is also relatively high or if the frequency and duration of power outages for that cabinet is also relatively high.

In addition, and in response to the argument above that there is limited benefit to providing back up at the cabinet if customer premises have no power, we also remind providers to consider that:

- Communications providers have an obligation under General Condition A3.2(b) to take all necessary measures to ensure uninterrupted access to emergency organisations as part of any voice communications services offered. Ofcom guidance on the measures providers should have in place to ensure customers making calls over broadband are able to make emergency calls in the event of a power cut at their premises sets out that providers should have a solution available that enables access to emergency organisations for a minimum of one hour in the event of a power outage in the

[101] Source: Ofgem data.
[102] Department for Energy Security & Net Zero, Electricity Supply Emergency Code: *An outline of the process for ensuring fair distribution of electricity rationing during a prolonged electricity shortage.* https://assets.publishing.service.gov.uk/media/65f8343f78087a001a59ebc0/esec-guidance-revised-november-2019.pdf

premises, and that this solution should be offered free of charge to those who are at risk as they are dependent on their landline.[103] Some providers of digital landline services offer an in-home power backup for their digital landline equipment and associated broadband equipment. These typically last for several hours;[104]

- Some customers may have supplied their own power backup solution within their premises and more customers may choose to do so in the future, particularly if they are aware that their provider has power backup at their local cabinet;
- In some scenarios, mains electrical power to a given premise could continue to function normally while there is a power outage to the active access network enclosure serving that premise. This is often the case with FTTP passive optical access networks where distance from powered network infrastructure to the premise can be much further in comparison with copper-based broadband access networks.

5.61 Based on the factors above, we would consider power backup with a planned capacity of 3 or 4 hours to be good practice for active fixed access cabinets that are new installations. In areas that suffer longer power outages more frequently, we would expect providers to consider an increase to the duration of power backup.

5.62 We note the points made about the environmental impacts that may result from the increased use of batteries to ensure mains power is adequately backed up. Given that existing cabinets would not be expected to be backed up as part of this guidance, the additional environmental impact would likely be minimal. The shift to using different types of networks, such as those highlighted in the responses e.g., FTTP Passive Optical Networks (PONs), means there are likely to be fewer active cabinets and therefore fewer batteries needed in future. We also point out that batteries are only one method to provide power back up, and other more energy renewable sources can also be employed over time, as noted by one respondent.[105]

5.63 We note the comments above, suggesting more could be done to encourage greater co-ordination between the power and telecoms sectors to support network resilience. Responses suggest more could be done to share the responsibility for reducing the impact of outages, and for providers to have priority for restoration of mains power to their networks. Ofcom is working with relevant government departments and other relevant organisations to encourage and support greater progress on these matters. We provide some further detail on our next steps in section 8.

Consultation proposals for measures at the Aggregation / Backhaul domain

5.64 As explained in the consultation, the aggregation/backhaul domain of a provider's network tends to comprise the intermediate links between the access network and the core network. The number of physical sites and geographical spread of the aggregation/backhaul domain are far greater than the core domain (discussed below); typically, by a factor of 100 to 1000 times greater.

---

[103] Ofcom, 2018: *Protecting access to emergency organisations when there is a power cut at the customer's premises, Guidance on General Condition A3.2(b)*.

[104] Virgin Media, *Everything you need to know about the digital voice switch over*; BT, *Digital Voice: Will my service still work in a power cut*

[105] Virgin Media O2 response to the consultation, p.15.

5.65 The proposed guidance (section 4.2.2) explained that significant numbers of customers can be impacted if a single aggregation node fails. This is because aggregation nodes combine the traffic from multiple access points. The proposed guidance highlighted the importance of examining resilience implications when making design decisions affecting the aggregation and backhaul domain. In particular, as the number of aggregated customers/premises increases at an aggregation point in a network, we would expect providers to adopt measures to address such risks. This includes measures such as enhanced onward connectivity and physical resilience, e.g., through equipment redundancy, separate transmission links and dual parenting.

5.66 The introduction of these types of resilience measures can be costly and providers may need to prioritise where they deploy them to have the most impact. The proposed guidance outlined the factors which providers should consider when deciding where best to deploy these resources. In particular, it set out that providers should consider Ofcom's 'user hours lost' reporting threshold when deciding at which sites to prioritise resilience measures, as this sets out our view of the level at which service impacts are likely to be significant.

Summary of responses to the proposed measures at the Aggregation / Backhaul domain

5.67 Some respondents raised issues about the power back up provisions at aggregation/ backhaul sites. Specifically, they argued that it was not proportionate to implement dual resilient mains electricity feeds here. Similar concerns were raised about Core back up, so we are covering our response to these points at paragraph 5.105 below.

User hours lost

5.68 Virgin Media O2 questioned the helpfulness of relying on the user hours lost threshold when deciding on which sites to prioritise for resilience measures. It argued there is no minimum threshold set out in the Procedural Guidance so how would a provider know if there is a trigger for prioritising one site over another.[106]

5.69 It also argued that it was not a suitable metric for mobile incidents, as user hours lost can only be calculated after an incident has taken place. It suggested that other factors may be relevant when selecting sites for additional investment. These include number of customers potentially affected (rather than user hours lost), as well as the consideration of alternative resilience mitigations, such as overlapping coverage in the event of a mobile incident.[107]

5.70 Virgin Media O2 also highlighted that Ofcom included a set of factors in its 2022 Guidance that is absent in the latest version, stating that it is unclear whether any of these factors would be relevant in the assessment of what is appropriate and proportionate, and this leads to uncertainty.[108]

Link Aggregation Group connectivity

5.71 Fibrus explained that it is planning to provide a service over Openreach's network, delivered by purchasing cable links between Fibrus' aggregation layer and Openreach's Optical Light Terminals. However, Fibrus stated that the product sold by Openreach does not allow it to provide resilience across these links. It added that if a link fails, service would

[106] Virgin Media O2 response to the consultation, p.19.
[107] Virgin Media O2 response to the consultation, p.19.
[108] Virgin Media O2 response to the consultation, p.19.

not be restored until the link is replaced by Openreach and it has asked Openreach to provide link aggregation group (LAG) connectivity for these cable links to ensure that there would not be a single point of failure.[109]

5.72 In its response, Openreach said that it offers multiple Cablelink products if required, which can limit the impact of any individual port failure, meaning the risk and potential impact is determined by providers' network architecture in terms of their Cablelink configuration and customer loading. It said also that it was considering the introduction of LAG functionality, but the provision of cost-effective protection for Cablelink connectivity is likely to require industry level agreement to find a solution.[110]

Assessment of responses to proposed measures at the Aggregation / Backhaul domain

5.73 Having considered consultation responses, we have decided to maintain the approach to the aggregation / backhaul domain in the Guidance.

User hours lost

5.74 Ofcom's Procedural Guidance contains qualitative criteria and numerical thresholds that set out Ofcom's view of which security compromises are likely to be significant and should therefore be reported to Ofcom. These thresholds are based on the minimum number of end customers affected by a service impact and its minimum duration.

5.75 Ofcom considers a service impact to be significant where the user-hours lost figure is equivalent to or above the *numerical threshold* set out in the tables for fixed and mobile in the Procedural Guidance which corresponds to the relevant network/service type. This user-hours lost threshold is calculated by multiplying the *minimum number of end customers affected* and the *minimum duration of service loss or major disruption for the voice or data service/network offered to retail customers*.

5.76 In the Resilience Guidance, the user-hours lost incident threshold calculations also serve as a target to remain below when providers are considering architectural, design and operational decisions, with particular focus on establishing where numbers of customers/premises increase at an aggregation point in a network and the level of risk associated with incidents that may occur.

5.77 We disagree with Virgin Media O2's point regarding user hours lost not being a suitable metric for mobile. MNOs can use network control plane monitoring to establish the number of customers impacted by an incident. This can be used as a basis to calculate user hours lost. We discuss our guidance on network control plane monitoring in section 6. The user hours metric can be used as a planning tool to assess which parts of the network require additional resilience measures, particularly in parts of the network that represent single points of failure. In this context, it can be used as a preventative tool, rather than something to be considered only after an incident. However, previous incidents, along with the other considerations that Virgin Media O2 set out, may also be relevant factors to consider as part of this process. It should be noted that the use of the user-hours lost

[109] Fibrus response to the consultation, p.3.
[110] Openreach response to the consultation, paragraph 23, p.5.

metric in this guidance to identify significant service disruption does not impact on any aspects of the incident reporting process itself.

5.78 Ofcom explored alternative options when setting out our approach to assessing resilience measures for single points of failure in a network in this guidance. This included examining the suitability of an 'absolute value' which would set a limit on the number of customers dependent on a single point of failure. We considered that this would be too inflexible because it is difficult to apply one rule to different technologies, which typically have different failure rates and/or repair times.

5.79 The 'hard rule' approach would necessitate designing a set of rules for different technologies, which would need to be regularly reviewed and may not be easily applicable to every type of technology, creating a lack of clarity and certainty for providers. Instead, we have opted for an approach which is outcome-based and provides more flexibility and can apply across all technologies with a single common approach. We feel this is the most suitable way to set our expectations on the steps that providers should take when considering where additional resilience should be prioritised.

5.80 Ofcom also contests Virgin Media 02's view that the removal of the set of more general considerations which are present in the 2022 Guidance makes it more challenging to assess what proportionate measures can be taken in relation to single points of failure.

5.81 While the considerations in the newly updated guidance are not provided in the same format as those in the 2022 Guidance, the broad themes noted in paragraph 5.39 of the 2022 Guidance are addressed individually in various parts of the document. For instance, "the number of customers relying on the single point of failure" is addressed in the Aggregation / Backhaul section in relation to user hours lost and provides greater detail than set out in the 2022 Guidance. The "geographic and physical constraints" is highlighted in section 3.3.1 of the Guidance, and we note the significance of emergency calls when highlighting resilience considerations for site and network design in section 4.2.1. Paragraph 5.40 of the 2022 Guidance included "*loss of service to a significant geographical area, potentially isolating whole communities*" which is reflected in updated text in section 4.2.1 of the revised guidance.

Link Aggregation Group connectivity

5.82 Openreach's general Significant Market Power obligations require it to provide access on reasonable request. If Openreach does not agree to Fibrus' request for a product with LAG functionality, Fibrus can consider whether this might form the basis of a complaint or regulatory dispute referral to Ofcom.

Changes included in the Guidance on measures at the Aggregation / Backhaul domain resulting from the consultation responses

5.83 For the reasons outlined above, we are maintaining our consultation approach in the Guidance to the aggregation / backhaul domain, including in respect of the use of the user hours lost metric. We do not believe it is necessary to change our overall approach of setting an expectation that providers should use the user hours lost metric when considering which parts of their network to prioritise for additional resilience measures.

5.84 However, we think that the proposed guidance could have provided more details about how the user hour lost metric was formulated and how it can be applied. As a result, we have added a worked example into the Guidance to provide greater clarity.

5.85 In addition, we do not believe that a return to the more general formatting of the 2022 Guidance is needed, as it would be an unnecessary duplication of information in other parts of the Guidance.

Consultation proposals for measures at the Core / Metro domain

5.86 The consultation explained that core connections and nodes carry multiple telecoms services to customers, and generally have higher capacity than their backhaul equivalents. Core nodes are used to route (or switch) traffic from backhaul connections onto the core network, or between backhaul nodes or other core nodes. Core sites host the provider's most critical network and service functions and are typically built to the highest standards of resilience practically and economically possible.

5.87 The proposed guidance (section 4.2.3) outlined a number of measures that providers are expected to take to ensure that resilience at the core is adequately prepared and maintained. These include ensuring that there are multiple separate physical links between different core sites so that traffic can be diverted when one or more core sites fail. In large scale networks, this could mean resilient connections to four or more other core sites. Larger networks containing metro sites would be expected to have resilient connections to at least three other metro or core sites using separate and diverse transmission. Communications providers would also be expected to ensure that all key network and service functions (discussed further below) can continue at alternative core sites if those functions can no longer be performed at the existing core site.

5.88 The proposed guidance also explained that these precautions should be supported by adequate forecasting and planning, to ensure that alternative sites can handle significant increases of inward network traffic, if needed, at short notice. The location of core sites should also be considered, so that areas with likely geological hazards (e.g., flooding) or patterns of extreme weather can be avoided where possible.

5.89 A further key risk at the core level identified in the proposed guidance is electrical power backup. Power outages at core sites can potentially affect millions of customers at any one time. Given the scale of potential negative impact, we explained that providers should be prepared for extensive outages. We therefore proposed that core sites should have adequate power backup to ensure services can be maintained for at least 5 days in the event of a power outage.

Summary of responses to measures at the Core / Metro domain

Core site terminology, applicability of metro to a range of providers' networks and resilient connections between core/metro sites

5.90 The responses indicated there may be several different interpretations of what 'core site' actually means. Interpretations vary depending on the size of a provider, and potentially on where the provider sits in the end-to-end network between end-users and the service application or content. The responses indicated that some of the expectations that we set

out for 'core' sites may not be practical or appropriate for sites that some providers appear to consider as their core sites.

5.91 Some providers disagreed with Ofcom's proposed meshed approach to resilient connections and questioned how it applied to different types of networks.[111]

5.92 BT argued that best practice would be connections to two metro sites, not three. It noted BT's dual core network means that if a metro site has connections to two other core sites, it actually has four separate connections.[112]

5.93 Sky suggested that the three-plus degree fibre connectivity from metro to core sites is unnecessary and that Ofcom should focus on supporting next generation upgrades to metro sites, where existing sites have appropriate alternative approaches to ensure availability. [113]

5.94 Virgin Media O2 argued the proposed meshed approach would not be cost effective or practical and if other measures, e.g., automatic failover between core sites, are in place then losing a site would not affect service availability for customers. It argued the guidance ought to make a distinction between physical diversity and logical diversity, providing the example that their mobile Core network works through logical resilience, not underlying meshed physical resilience, which we believe ought to be a factor in what diversity is appropriate and proportionate.[114]

5.95 CityFibre suggested their fibre exchanges have redundant connectivity by design and it was unclear whether their fibre exchanges fell into the 'core/metro' domain. It argued that if it did, a meshed architecture with four connections to other core sites would add little resilience and substantial costs. [115]

Power back up measures at core sites

5.96 Several respondents expressed concerns about the proposed measures aimed at improving electrical power resilience at core sites. In particular, the proposal at 4.2.3 that 'Electrical power provision at each core site is expected to include the following as a minimum: dual resilient mains electricity power feeds, battery backup, and fuel-powered electricity generators.'

5.97 Several respondents, including INCA, explained that the addition of dual resilient mains electricity power feeds to core *and* aggregation sites was not practical. Issues such as cost, proportionality and availability were cited, and in addition the fact that power backup would already be secured by a battery/UPS and fuel powered electricity generators.[116]

5.98 One respondent questioned whether requiring 5 days back up at core sites was excessive.[117]

---

[111] INCA response to the consultation, p.5.
[112] BT response to the consultation p.14.
[113] Sky response to the consultation p.2.
[114] Virgin Media O2 response to the consultation, p.20.
[115] CityFibre response to the consultation, p.4.
[116] BT response to the consultation p.15; CityFibre response to the consultation, paragraph 10; [✂] response to the consultation, paragraph 2, p.5; INCA response to the consultation, paragraph 37; ISPA response to the consultation, p. 6-7; Sky response to the consultation p. 5.; UKCTA response to the consultation, paragraph 13; Virgin Media O2 response to the consultation, p. 11-13.
[117] [✂] response to the consultation, paragraph 10.

5.99 Other respondents mentioned that some key geographical sites were located in data centres and sought clarification about whether engaging the services of a reputable datacentre provider, who offers suitable power back up assurances, would satisfy the requirements.[118]

5.100 Comms Council UK stated that some of its members have struggled to engage meaningfully with relevant government departments responsible for civil contingencies and asked Ofcom to ensure that diesel deliveries are provided for all Electronic Communications Network /Electronic Communications Service providers in the event of lengthy outages that impact core networks.[119] [120]

Ofcom assessment of responses to proposals for measures at the Core / Metro domain

5.101 Again, we have decided overall to maintain our consultation approach in the Guidance, subject to a few clarificatory changes to address stakeholder comments as explained below.

'Core site' terminology

5.102 We want to ensure clarity and consistency on the definition of a core site, which is expected to apply to a small number of sites. We have updated the text describing the 'core' domain to reflect that it is a small number of sites containing critical network functions or having critical importance.

5.103 We recognise providers' concerns about the applicability of guidance on the previously described 'metro' sub-domain to their variety of site topologies. These sub-domains are typically only found in larger networks and not intended to apply to all types and sizes of network. For clarity and to ensure the guidance is directly applicable to a broad range of networks, we have removed the optional 'metro' sub-domain from the guidance.

5.104 We recognise providers' concerns that 'four or more' connections between core sites in large networks could be impractical and costly, and have changed this to refer to connections between 'multiple' other core sites instead. We consider that, having made the changes to reflect providers' concerns, the measures are appropriate and proportionate to ensure resilient, physically separate, diverse connections, given the importance of core sites.

Power backup measures at core sites

5.105 When considering power backup measures at core sites, we are mindful of the scale of harm to end users that may result if mains power is lost. The risk of broader catastrophic network failure is dramatically increased during an mains outage. As explained at 5.89, the loss of a core site has the potential to impact millions of end users, so we consider that it is appropriate to implement measures to ensure continued operation in the event of power loss from the electricity grid. The Electricity System Restoration Standard requires the Electricity System Operator (National Grid ESO) to have sufficient capability and

[118] CCUK response to the consultation, paragraph 10; County Broadband response to the consultation P.1. Magrathea response to the consultation p.1.
[119] CCUK response to the consultation, p.11.
[120] A definition of "Electronic communications network" is set out in section 32 of the Communications Act 2003.

arrangements in place to restore 100% of Great Britain's electricity demand within 5 days.[121]

5.106 We therefore consider it is appropriate to expect providers to be able to provide power backup at core sites for up to 5 days, as a minimum, to cover this intervening period. We have not received any information during this consultation exercise to change our view that having the capability and arrangements in place to ensure power backup at core sites for up to 5 days is good practice. Therefore, we continue to view this as appropriate and proportionate practice for core sites.

5.107 We have carefully considered the responses about the proposal to include 'dual resilient mains electricity power feeds' at each core site and aggregation site. Our review of these responses indicates that this specific measure is not a consistent practice.[122] We also recognise concerns that implementing these measures retrospectively would incur significant costs and might not necessarily enhance overall resilience. On the basis that respondents have highlighted that other essential provisions including battery backup (UPS) and fuel-powered electricity generators are available at these sites, we have not included the 'dual resilient mains electricity power feeds' measure in the Guidance.

5.108 We note some respondents explained that some aspects of their network infrastructure are located in data centres and asked whether using a datacentre provider who offers suitable power back up would be appropriate. We acknowledge that this approach may provide a cost-effective way to achieve appropriate resilience, and have added some additional text in section 3.3 of the Guidance to confirm this.

5.109 Ofcom does not have a role in the fuel priority scheme, which is administered by government and is outside the scope of our guidance. Therefore, we would encourage industry to engage with the government directly about the eligibility criteria. However, we understand that the designation of fuel in applicable scenarios covers 'field force' vehicles rather than the provision of diesel for backup generators. Irrespective of the Government's fuel priority scheme, all providers should ensure that they have their own processes in place to ensure that core sites have adequate power backup to ensure they can maintain services of at least 5 days in the event of a power outage, given these types of outages can affect millions of customers at any one time.

Changes included in the Guidance for measures at the Core / Metro domain resulting from the consultation

5.110 The final guidance covering resilience measures at the Core will be the same as that proposed in the consultation apart from the following changes to reflect the decisions we have explained above:

a) We have clarified in section 3.3 the brief description of core sites to read 'Core: small number of sites containing critical network functions or having critical importance'. There is also an update to the expanded description in section 3.3.3 of the Guidance.

[121] ESO. Electricity System Restoration Standard. https://www.nationalgrideso.com/industryinformation/balancing-services/electricity-system-restoration-standard [accessed 5 December 2023].

[122] The exception appearing to be BT, who stated it uses dual mains feeds at some core sites.

b) Reference to ‘metro’ sites has been removed from the guidance text and diagrams;
c) Reference to ‘dual resilience mains electricity power feeds’ has been removed;
d) Reference to a ‘significant amount of resilient connections’ between core sites meaning that in large scale networks, this could involve ‘four or more’ connections has been removed. It has been replaced by reference to ‘multiple’ other core sites (in large scale networks).

Consultation proposal for measures at Internet Peering and non-Internet Interconnection domain

5.111 To enable customers on different networks to communicate with each other, or to access services, networks are usually interconnected between, or near to, core nodes. The network-to-network interconnect may be at a site (point-of-handover) where both networks are present, such as a large regional exchange, data centre, or at an internet peering site or other form of co-location exchange point. In some instances where two networks are not co-located, interconnect may be achieved using dedicated point-to-point connections between the two networks’ sites.

5.112 The proposed guidance (section 4.2.4) explained that a failure to consider resilience at the peering and interconnect domains could result in a loss of services to end users e.g. prevent a person calling another person using a different network, or access a resource or service hosted on a different network. The proposed guidance outlined a number of measures that we expect providers to take to ensure that resilience at the peering and interconnect domain remains robust. This included: use of multiple geographically separate paths to third-party networks with appropriate capacity to ensure services run well even when one or more links fail, and that non-Internet interconnection between networks (such as voice interconnection) should be separate from the Internet. We explained that providers should also consider physical and logical routes connecting networks beyond the UK, including subsea cables.

Summary of responses to proposed measures at Internet Peering and non-Internet Interconnection domain

5.113 Some respondents, who supply services in the voice market, expressed concerns with the proposals to separate interconnections from the wider internet.

5.114 Voxyonder argued that the many smaller providers use the public internet for interconnection. It argued that, as each of these smaller providers conveys relatively small volumes of voice calls, it is an appropriate and proportionate method of doing so. It suggested that any attempts to prevent providers from using this method could disrupt existing business models, reduce innovation, and stifle competition in certain parts of the voice market. Further, that there are various mitigation steps that can be taken so that providers can use the public internet for interconnection and still meet the overall resilience objectives.[123] In particular, Voxyonder made reference to the Security Regulations and Security Code of Practice (described above at 3.9) that, among other things they state, require certain providers to introduce encryption practices.[124]

[123] Voxyonder response to the consultation, p.2.
[124] The Electronic Communications (Security Measures) Regulations 2022, 4(5); DSIT, 2022: Telecommunications Security Code of Practice: (Paragraphs 3.28-3.30).

5.115 Magrathea acknowledged that, where proportionate (e.g. for critical services), the interconnection service should not be reliant on the wider internet and vital (e.g., tier 1 carrier grade) interconnect arrangements should be dedicated to the exchange of voice traffic between two parties. However, it also noted it had encountered many situations where they would consider it proportionate and appropriate to interconnect via links which would be considered internet based, and so enable a wider number of service providers to access core networks at competitive rates, with fewer barriers. It maintained that while these links do share traffic with other service types, they are still specified and engineered with the voice traffic in mind and often never enter what might be considered the general internet, as traffic is exchanged between the two networks at an interchange point such as LINX. It argued that for lower call volumes and non-essential services provided to a sub-set of end users, the impact is generally manageable in the event of an internet related issue. To introduce onerous obligations on these smaller providers would stifle innovation, reduce competition, and increase costs for consumers. [125]

5.116 BT said that 'Ofcom's updated guidelines on Net Neutrality state that providers can use "reasonable" traffic management measures to contribute to an efficient use of network resources, ensuring appropriate capacity. And "exceptional" traffic management to preserve the integrity and security of the network or mitigate the effects of network congestion. We [BT] suggest that Ofcom acknowledges there are other methods to ensure there is sufficient capacity in the network in its final resilience guidance.'[126]

Assessment of responses to measures at Internet Peering and non-Internet Interconnection domain

5.117 Broadly, we have decided not to make significant changes to the proposed measures relating to internet Peering and non-internet interconnection domain.

5.118 We note the argument that smaller providers convey relatively small volumes of voice calls and that conveyance over the internet is an appropriate and proportionate method of doing so. Ofcom acknowledges that some providers handle relatively lower call volumes at the voice interconnect domain compared to larger operators. However, where critical voice calls may be being handled, we do not accept that relatively small-scale operations carry less risk and should be exempt from these resilience measures if they fall under a certain threshold. While the potential volumetric impact of resilience failures might correlate with call volumes handled, we consider it appropriate that certain standards of resilience should apply to all providers that handle voice calls, regardless of quantity. There is no guarantee that the nature of these calls would not be critical, such as emergency calls. Furthermore, collectively, these smaller providers may handle significant proportions of overall industry call volumes. Therefore, Ofcom expects all relevant providers to consider minimum resilience standards, irrespective of the call volumes they handle.

5.119 We note the point made about the Security Code of Practice, and the additional protections that might result from the introduction of certain encryption practices. The argument being that encryption could greatly reduce the risk of 'cyber security' related security compromises on voice services that run over the internet, in relation to confidentiality and integrity. We agree that encryption serves an important role in reducing certain types of

[125] Magrathea response to the consultation, p.1-2.
[126] BT response to the consultation, p.18.

security compromise. However, we do not accept that these encryption measures will address the full range of 'resilience-related' security compromises that could occur at the interconnect domain that would fall under the scope of sections 105A-D. The measures included in the Guidance seek to address resilience and reliability aspects of voice services and interconnection that are not necessarily a result of malicious cyber-attacks. These aspects are not addressed in the Security Code of Practice which is primarily concerned with cyber-security.

5.120 We also note the point made that many, potentially hundreds, of smaller providers currently use the internet as a method for facilitating interconnection for voice services and the concerns that these providers could be adversely impacted by the measures included in the guidance.

5.121 However, in our view, providing critical voice services to end users that run over, are dependent on, or exposed to, the wider public internet gives rise to various risks of malicious and accidental outages and impairments; 'security compromises' in this context. This is because the internet's open nature creates a complex support environment with inherent limitations that may present a number of challenges to providers, these include:

a) the internet lacks a coordinated support structure and standardised cascading service level agreements (SLAs). This makes it difficult for providers to guarantee consistent performance and troubleshoot issues efficiently;

b) while the internet fosters accessibility, it also facilitates accidental disruptions and malicious activity. Accidental routing errors and advertisements can significantly impact service, and sometimes these issues lie outside a provider's direct control, hindering rapid service restoration;

c) distributed Denial-of-Service (DDoS) attacks are a persistent threat, as evidenced by the attacks on OTT VoIP providers in the UK (as highlighted in the Connected Nations 2021 report). These attacks can severely disrupt services, causing significant downtime and customer frustration; and,

d) due to the inherent lack of trust within the internet, providers typically remove differentiated service priority markings from data packets upon entering their networks. This eliminates the ability to prioritise critical services such as voice calls or emergency communications.

5.122 We consider that these risks can only be addressed by providers not using the public internet as a method of interconnection between networks for voice calls, as to do so would be to increase risks to the performance and functionality of voice services.

5.123 We also consider that providers can take measures to facilitate the interconnection of voice calls in a way that it is resilient which does not generate adverse costs that which are disproportionate to the aim pursued.

5.124 For example, providers often have some form of presence in co-location/tele-hotel interconnection sites and could make use of infrastructure or services within those sites to interconnect to other providers in a way that is either physically or logically separate from internet traffic and the wider Internet. We note that Magrathea refers to a similar set of measures within its response: '*Whilst these links do share traffic with other service types, they are still specified and engineered with the voice traffic in mind and often never enter*

what might be considered the general internet, as traffic is exchanged between the two networks at an interchange point such as LINX'.[127]

5.125 We are aware of alternative measures that can be taken to support a good level of resilience for voice interconnection. For example, in response to Ofcom's Wholesale Voice Markets Review, industry respondents who also raised concerns about the risks of voice interconnection over the internet, noted that a number of steps could be considered to ensure that providers interconnect securely, including:

i) private direct interconnects,
ii) IP peering at a UK internet exchange,
iii) or a private VLAN at a UK internet exchange.[128]

5.126 Whilst we do not consider it is appropriate to specify any particular measure, our view is that any, or a mix of, the measures above would be likely to represent appropriate measures to support a good standard of resilience. By taking such measures, providers could achieve an interconnection model which supports reliable service levels, and protects the voice service from DDoS and other malicious attacks, with an operational model which supports robust connectivity monitoring and timely service restoration following resilience incidents.

5.127 We acknowledge the costs associated with meeting certain interconnection resilience standards, and this may impact some current provision, however we consider these measures remain appropriate and proportionate. As an example, we would expect that the most significant driver of costs to a provider would be the service fees charged for locating their own infrastructure to a data centre. Our own desk research suggests that, in the UK (London), the costs to a provider to locate a small amount of interconnection equipment in a data centre along with local connectivity to other providers would range from £200 to £600 per month.[129] In order to support good resilience for peering activities, we expect providers to locate in at least two co-location/data centres. Based on this evidence, our view would be that it is possible to take measures that would not generate a disproportionate level of costs given that a resilient critical voice call could prevent the loss of human life, which is often valued in the millions. [130] That is, we consider it proportionate to reduce the risks to the performance and functionality of voice services as articulated in paragraph 5.121 above.

5.128 We are also mindful of the points made about the risks to competition if providers exit the market as a result of this guidance. Ofcom are due to launch the next Wholesale Voice Markets Review in due course, and this will provide a timely opportunity to review these matters in further detail.

---

[127] Magrathea response to the consultation p.1.
[128] Ofcom: *Wholesale Voice Markets Review 2021-26*, Statement. Paragraph 9.27.
[129] WIK-Consult report (2022): Competitive conditions on transit and peering markets (p.49). According to the WIK Study, prices for public peering typically consist of one-time fees for connection to the IXP and a monthly fee per port used (with a maximum capacity for data traffic per period of time). WIK updated a previous price comparison across EU member states, but including the UK, prepared by the Dutch regulator, ACM. According to this, the monthly lower and upper bound prices in London for a 10 GE/Gbps port were €268-720 (converted to £230-617 in August 2024).
[130] University of Bristol, 2018. *Calculating the value of human life: safety decisions that can be trusted.*

Changes included in the Guidance at Internet Peering and non-Internet Interconnection domain resulting from the consultation

5.129 As explained above, we have decided not to make significant changes to the proposed measures relating to internet Peering and non-internet interconnection domain. However, we have decided to include some additional text to highlight the importance of providers having an appropriately robust operational model to ensure timely fault detection and restoration. This is an important consideration given these voice interconnects may carry emergency calls and other essential calls.

5.130 We have also added some additional text to 4.2.4 to address BT's point about the existing provisions in the Net Neutrality guidelines for 'exceptional' traffic management.

Decision on resilience measures at the physical infrastructure domain

5.131 We consider that the decisions we have taken in the Guidance on the physical infrastructure domain, as set out above, are appropriate and proportionate.

5.132 Our aim is to implement guidance which seeks to secure the provision of networks and services which are robust, available, and working well, both in the provision of voice calls and the provision of internet access services generally, ensuring an appropriate level of resilience for consumer services across the UK.

5.133 We have concluded that the measures set out in the Guidance for network infrastructure domains are appropriate to achieve this aim as, if these measures are not taken by providers, there is an unacceptably high risk of significant loss of connectivity for end users. In designing this guidance relating to the physical infrastructure domains, we have drawn upon a number of best practice documents that have been developed over time by several different standards bodies and industry working groups, as well as Ofcom expertise in industry.

5.134 Of particular relevance to the network infrastructure domains of a network is the existing EC-RRG Resilience Guidance ('*EC-RRG Guidance*').[131] The Electronic Communications Resilience & Response Group (EC-RRG) is a cross government and telecoms industry forum whose aim is to ensure the telecoms sector remains resilient to threats and risks to services. EC-RRG represents all elements of communications services in order to promote resilience across the sector.

5.135 The Guidance makes clear that we expect providers to give appropriate consideration to minimum standards and practices which apply to the resilience of network infrastructure and incorporate such measures into their networks where appropriate. The Guidance also reflects some of the design recommendations included in the EC-RRG Guidance which relate to a number of aspects of network resilience, which we consider are not simply good practice, but represent the minimum set of measures which we would expect providers to take in order to meet their resilience-related security duties.

[131] DSIT & DCMS, 2022. *Guidance, Electronic Communications Resilience & Response Group (EC-RRG).* https://www.gov.uk/guidance/electronic-communications-resilience-response-group-ec-rrg [accessed 22 November 2023]

5.136 The EC-RRG Guidance advises providers to assess the risks and invest, where practical, in duplicate or triplicate backups for their equipment ('redundancy') and in diverse transmission routings.[132] Further, it recommends that providers build redundancy in network design so that backup systems are available to duplicate the functionality of systems that would otherwise not be available to take over in the event of failure.[133] We consider that the measures included in the Guidance, relating to the physical network domains, are already recognised within established industry standards as being appropriate for the provision of robust and resilient networks and services. We therefore consider it is appropriate to include reference to the consideration and appropriate inclusion of such measures in the guidance.

5.137 The guidance relating to the physical infrastructure domains has also been developed with a consideration of recent experience of real-world provider network failures and outages captured as part of Ofcom's own incident reporting regime. These examples serve to illustrate where weaknesses in networks and services may lie, and the real-world effects of resilience failures in the network infrastructure domain.

5.138 For example, one of the UK MNOs had a power failure within one of their core sites. This resulted in a complete core site outage. The core site was connected to the MNO's 4G RAN (or mobile mast) sites. But these mobile sites were not configured to connect to an alternative core site if the current core site had an outage. As such, all mobile sites, connected to the affected core site, were unavailable until the cause of the issue at the core site was resolved. This resulted in an outage at 582 mobile sites for 0.25 hours. The MNO has since reconfigured their mobile sites to connect to an alternative core site if the primary core site experiences an outage.

5.139 Between September 2022 and August 2023, Ofcom noted 1076 incidents reported to us related to the access domain, these had a total impact of 54 million customer-hours lost across fixed and mobile services. This demonstrates the scale of impact when aggregated. Conversely, a single reported incident in the interconnect domain affecting a number of providers generated a loss of almost 15 million customer hours, across 3 days.

5.140 There are also examples from outside of the UK, including the US, where providers have experienced significant issues that may have been avoided if the practices outlined in the guidance had been followed. We believe that these are relevant as the technology behind, and design of, networks in the US are very similar to those used in the UK.

5.141 On June 15, 2020, the US provider, T-Mobile, experienced an outage on its wireless networks that lasted over twelve hours. The Federal Communications Commission's ("FCC") Public Safety and Homeland Security Bureau estimates that at least 41% of all calls on T-Mobile's network failed during the outage, including at least 23,621 failed calls to 911.[134] Following its investigation into the causes of the incident, the Bureau identified several network reliability best practices that could have prevented the outage or mitigated its effects, including communications providers periodically auditing the diversity of their

[132] EC-RRG, 2021. *EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure*. p13. Section 7.1.5.
[133] Ibid. p19-20. Section 8.1.1.5.
[134] Federal Communications Commission, 2020. *FCC ISSUES STAFF REPORT ON T-MOBILE OUTAGE Investigation Identifies Measures to Prevent Similar Outages in the Future*

networks. Of particular relevance to the measures outlined in the proposed guidance was the following FCC recommendation:

'*Network operators should periodically audit the physical and logical diversity called for by the design of their network segment(s) and take appropriate measures as needed. T-Mobile could have prevented the outage if it had audited its network during the new router integration to ensure that the traffic destined for the failed link would redirect to a router that was able to pass it. If the backup route had operated as it was designed, a nationwide outage would likely not have occurred.*[135]

The incident above, and the lessons noted in the official report, are applicable to networks in the UK. They serve as a useful reminder of the importance of including physical and logical diversity into network design to reduce the risk of outages.

5.142 These experiences, and particularly the impact that these have had on end users, further strengthen our view that the requirements included within the Guidance are appropriate.

5.143 We also consider that the measures set out for the network infrastructure domains are proportionate as they go no further than is necessary in our view to provide an appropriate level of resilience, including providing flexibility where appropriate.

5.144 In preparing the detail of the guidance, Ofcom has been mindful to avoid overprescribing how providers design, build, and operate their networks. Instead, we have sought to ensure that providers are able to refer to the guidance measures to help them assess what steps are necessary, based on the circumstances of any given use case. For example, while we expect providers to protect onward traffic flows from aggregation sites towards the Core, we do not necessarily expect providers to implement dual parenting or automatic failover measures at every part of the fixed access networks e.g., those parts that serve relatively low numbers of users. The exception to this approach is with power back up at core sites, where we suggest minimum power back up time periods (i.e., 5 days).

5.145 We consider that this general approach allows providers to implement measures which are necessary to fulfil their security duties under s105A-D in a given instance. To assist providers in assessing when and where they should deploy resilience measures, we provide more detailed guidance about where certain measures are more likely to be necessary, e.g., when user hours lost reporting thresholds are triggered. Our intention here is to provide a recognised method for providers to follow that enables them to decide where resilience measures should be prioritised but still allow for a reasonable degree of flexibility in their resilience planning.

5.146 We also consider that the measures set out for the network infrastructure domains will not produce adverse effects which are disproportionate to the aim pursued.

5.147 Over the last two years, Ofcom has undertaken significant engagement with providers to understand how their infrastructure at the various domains has been set up and operates in relation to network and service resilience. These engagements included all of the major fixed and mobile operators, plus a cross section of smaller communications providers that operate with relatively smaller user bases, e.g., alternative network providers. We understand from these engagements that most of the more detailed specific measures included in the guidance are already implemented by most of these providers. We have also

[135] Federal Communications Commission, 2020. *June 15, 2020 T-Mobile Network Outage Report*. p.16 paragraph 45.

undertaken a detailed public consultation on proposed guidance on measures relating to the physical infrastructure domain.

5.148 As such, our view is that providers who follow this guidance are unlikely to incur significant additional costs.

5.149 In some cases, the additional costs incurred could be significant, but we expect the benefits to be proportionally greater, such that the benefits still outweigh any significant costs.[136]

5.150 We further note in this respect that the guidance is not the only way for communications providers to comply with their resilience-related security duties under s105A-D. A provider may choose to comply with their resilience-related security duties by adopting different technical solutions or approaches to those specified in the guidance. What is appropriate and proportionate will depend on the particular circumstances of the provider.

[136] For example, the cost of ensuring a resilient core network in line with our guidance could be significant, but it is also likely that improving resilience in the core would have a greater impact on reducing the number of customer hours lost.

6. Resilience measures for logical planes and services

Summary

6.1 In this section, we present our analysis and conclusions on those resilience measures that relate to the control plane, management plane, and providers' own managed services, including voice telephony.

6.2 In summary, we have concluded that most of the measures outlined in the proposed guidance should be retained in the final resilience guidance. We have decided, following consideration of consultation responses, to provide some additional text to address some queries raised about the proposed guidance on the control plane and management planes.

6.3 We have also made more significant changes to the text relevant to the provision of voice services. This is intended to avoid overly restrictive measures whilst maintaining good resilience practices.

6.4 We provide a reminder of what measures were proposed, summarise respondents' views on them and explain our final decisions and why we consider they are appropriate and proportionate.

Control Plane Resilience

Consultation proposals

6.5 In networking terminology, the term 'plane' refers to a functional layer within the network architecture, where certain key processes take place. Two of the most commonly referenced planes in networking are the control plane and the management plane. We cover both of these terms below.

6.6 The control plane is the part of a network that is responsible for making decisions about how data is routed and processed by the user plane. The control plane does this by exchanging control messages with user plane devices, such as routers, switches, and other network functions that are typically part of networks. The software that runs on these user plane devices is also connected to the control plane. The control plane functions are critical, as the stability and correct running of the whole network is dependent on it working effectively.

6.7 The proposed guidance explained (section 4.3) that providers should take extra care to ensure extreme reliability/resilience in the design of the network control plane(s). The proposed guidance stated that we would expect providers to take measures to eliminate any service impacts if one or more of the instances of the special control plane functions relating to control plane scaling and overload resilience was to fail, malfunction, respond with unexpected errors, or become overloaded. It also said providers would be expected to implement appropriate signalling gateway and interconnectivity frameworks and associated overload control mechanisms.

6.8 The proposed guidance set out a number of measures that we proposed providers should consider to enhance resilience at the control plane (section 4.3.1). This includes designing the control plane so that:

a) it can continue to function even if one or more of the control plane processes fail;[137]
b) if important control plane functions fail at one point of the network, for example at a core site, they should also be able to switch to another location automatically to ensure continuity of services;
c) it can handle overload conditions and be robust enough to withstand a wide range of abnormal messages and conditions.

6.9 The proposed guidance noted providers would also be expected to take measures at the control plane to:

- avoid signalling overload at Customer Premise Equipment (CPE), and other user equipment (4.3.2);
- ensure that network functions with 'real-time charging' interfaces take resilience and reliability into account in their designs and testing (4.3.3); and
- ensure resilience and reliability are included in the design and testing of all aspects of the policy control solution and connectivity, including implementation of geographic separation of resilient instances with multiple parallel logical connections between components (4.3.4).

Summary of responses to the proposed measures at the Control Plane

Overall approach

6.10 Respondents who chose to comment were generally supportive of Ofcom's approach to control plane resilience. Several queries were noted relating to specific details of the proposed guidance.

6.11 Gamma explained that it already employs the principles outlined in 4.3 of the proposed guidance[138] and Three confirmed it broadly agreed with it.[139]

6.12 [✂] and Voxyonder both considered the guidance relating to the control plane was appropriate and proportionate.[140] SynOptika also agreed it was appropriate and proportionate but queried how it would be enforced. [141] Openreach supported the approach to control plane resilience. [142]

6.13 Three suggested Ofcom clarify that references to GSMA and NICC standards for Signalling Interconnection and Interconnection Connectivity Frameworks are to be used as guidelines and not technical specifications that providers will be audited against[143].

Eliminating service impacts

[137] This could be done by ensuring that control plane functions are situated across different locations, each with multiple active connections.
[138] Gamma response to the consultation, p.4.
[139] Three response to the consultation, p.6.
[140] [✂] response to the consultation, p.2; Voxyonder response to the consultation, p.1.
[141] SynOptika response to the consultation, p.2.
[142] Openreach response to consultation, p.6.
[143] Three response to the consultation, p.6.

6.14 The proposed guidance noted that "we would expect providers to take measures to eliminate any service impacts if one or more of the instances of these special control plane functions was to fail, malfunction, respond with unexpected errors, or become overloaded". Three suggested "or more" should be removed as networks are not designed to ensure no service impact in the case of multiple failures. [144] BT suggested it was not possible to 'eliminate' all service impacts or possible failure modes. [145]

Border Gateway Protocol (BPG)

6.15 Sky said the proposed guidance was selectively prescriptive, calling out isolated specifics such as BGP features, and should instead allow for appropriate and proportionate steps to be taken. [146]

Abnormal messages and unexpected conditions

6.16 Three suggested that the text 'ensuring all aspects of the instances and their feature set are hardened to be robust against a broad range of abnormal messages and unexpected conditions' should be taken out of the guidance. They argued this should be the responsibility of equipment suppliers, as operators typically do not have access to the code of products to verify robustness and it is not possible for operators to simulate these events in a test bed. [147]

Customer Premises Equipment (CPE)

6.17 BT agreed that it was important to protect networks against an overload of the network authentication mechanism but noted that providers may have limited visibility or control where customers have opted for third party customer premises equipment (CPE). BT argued the most effective control that protects the network against overload in these instances should be at the network edge, rather than in CPE. [148]

Policy Control Resilience

6.18 County Broadband noted that it would be difficult for Alt-nets to deliver the measures outlined on Policy Control Resilience, namely that measures 'should include implementation of geographic separation of resilient instances with multiple parallel logical connections between components.' [149]

Domain name systems (DNS)

6.19 In Section 4.3.6 of the proposed guidance, we noted we would expect providers to implement separate infrastructure resources with appropriate level of protection or isolation from each other, for customer facing domain name systems (DNS) and infrastructure facing DNS.

6.20 BT suggested that future models for DNS will not be physically separate as it will likely move to shared cloud infrastructure. BT suggested that Ofcom acknowledges that it is likely there

[144] Three response to the consultation, p.6.
[145] BT response to the consultation, p.16.
[146] Sky response to the consultation, p.6.
[147] Three response to the consultation, p.6.
[148] BT response to the consultation, p.16.
[149] County Broadband response to the consultation, p.2.

will be shared cloud infrastructure in the future.[150] Sky argued providers must be given sufficient time to implement this segregation.[151]

Ofcom assessment of responses to proposed measures at the Control Plane and changes made to these proposals

6.21 Overall, we have decided broadly to maintain our approach to the control plane in the Guidance. We describe below those changes we have made to the measures included in the final version of the Guidance.

Overall approach

6.22 We note the request for clarification on whether references within the Guidance to GSMA and NICC standards for Signalling Interconnection and Interconnection Connectivity Frameworks should be interpreted as guidance or service specifications that would be subject to future audits by Ofcom.

6.23 We have referenced international standards in the context of the Guidance, including from the GSMA and NICC, because they have been developed by industry over time and represent examples of good practice and are used by providers across the world. However, while the international standards themselves are illustrative of the types of approaches that would be consistent with our guidance, they do not themselves form part of the guidance.

Eliminating service impacts

6.24 We note some respondents requested some aspects of the proposed guidance be edited to reflect their view that the design and build of each network's control plane is different and the resilience measures should reflect that. They argued therefore that the final guidance should not include the degree of detail specified in the proposed guidance. Examples they cited include that [*measures are taken to prevent*] 'more than one' instance of control plane function failure. Or that [*measures are taken*] to manage 'any' subsequent service failures.

6.25 We agree that different control plane arrangements are likely to be in place for each type of network and we have revised the wording to remove the specificity included in the proposed guidance, so it is clearer that providers need to determine what control plane arrangements are appropriate. We draw attention to what we regard to be examples of good practice so providers have clarity on what measures they can take to avoid the risk of failures in the control plane functions and reduce any impact on services or customers.

Border Gateway Protocol (BGP)

6.26 We note Sky's comment above that the measures included in the proposed guidance can be selectively prescriptive on occasion – specifically those relating to BGP. As explained in paragraph 1.1. of the proposed guidance, we have set out our expectations in terms of 'outcome-based principles' but accompanied these with more specific measures including examples 'where needed.' We consider that special attention does need to be drawn to measures on BGP because:[152]

a) BGP is widely used, and the guidance relating to it will be relevant to the vast majority of networks in the telecommunications sector; and

[150] BT response to the consultation, p.16.
[151] Sky response to the consultation, p.6.
[152] We would note that the BGP guidance does not include specific measures in relation to every possible use case, as that would be impractical.

b) it is of critical importance to the smooth running of the rest of the network, and it could have catastrophic consequences for large sections of end users if BGP performance issues or failures occur. This is because reconvergence times could have significant impact on the control plane of other network functions running on or interacting with the IP network, in addition to direct impacts to customer or service IP traffic.

6.27 For these reasons, we maintain our view that it is appropriate to highlight these examples of good practice and have not made changes to this aspect of BGP guidance. We would remind providers that they can choose to comply with their security duties by taking measures different to those specified in the guidance.

Abnormal messages and unexpected conditions

6.28 We note Three's request that the text "ensuring all aspects of the instances and their feature set are hardened to be robust against a broad range of abnormal messages and unexpected conditions" be removed from the Guidance, as it argues that operators do not have access to the underlying code that would potentially enable them to take such precautions. Providers have a duty to take measures to identify, prepare for and reduce the risk of "anything that compromises the availability, performance or functionality" of the network or service occurring. Providers are not necessarily expected to have access to underlying vendor software code. However, we would expect providers to make appropriate technical assessments when selecting solutions and vendors for network functions. We also expect providers to ensure appropriate staff training and skills as part of ensuring appropriate design, configuration and testing of network functions individually and as an end-to-end network solution. For example, when considering a new solution, if a provider cannot get sufficient confidence from a vendor based on its technical assessment, this should be factored into any additional testing, optimisation, build, training and spend requirements on systems in test environments.

Customer premise equipment (CPE)

6.29 We recognise BT's concern that customers may have third party customer premise equipment (CPE) which is outside of the provider's visibility or control. We have amended the Guidance to reflect this limitation, and the measures only apply to scenarios where CPE forms part of the PECN/S.

6.30 We consider that where CPE devices host a provider's embedded services, such as a voice/TV/video client, those devices should represent the provider's network edge, in terms of service endpoints and associated control-plane and user-plane. We agree that controls should also be performed on the 'network edge' where the 'edge' is not on the CPE, but on functions deeper within the provider's network. A bullet point has been added to section 4.3.1 in relation to this.

Policy Control Resilience

6.31 In response to County Broadband's concern about Alt-Nets' ability to deliver the measures in the Policy Control Plane section, we would note that these measures are limited to mobile networks and not intended to apply to fixed networks.

6.32 We have not made changes to this aspect of guidance.

Domain name systems (DNS)

6.33 We recognise the points raised by BT and Sky about the general move towards virtualised and cloud-native solutions using a Network Functions Virtualisation Infrastructure (NFVI) based approach for many network functions. Resource separation is typically achieved in

virtualised or cloud-native implementations using anti-affinity rules. Anti-affinity rules are a standard approach in virtualised and cloud-native implementations to ensure that specified virtual machines (VMs), virtual network functions (VNFs), or other specific workloads do not share common hardware resources or interfaces such that failure or overload of one does not affect another. This capability is part of the standardised ETSI NFV-MANO model[153] and is also supported in Kubernetes container-based solutions[154].

6.34 Thus, we consider it appropriate and proportionate to ensure the separation stated in the Guidance is applied to key network functions (such as customer-facing vs infrastructure DNS) as part of their resilience mechanisms and logic.

6.35 We have retained the original text that applies to DNS. However, we have added text and references explaining the separation and anti-affinity capabilities in virtualised and cloud-native implementations.

Decision on resilience measures at the control plane

6.36 We consider that the decisions we have taken in the Guidance on measures at the control plane, as set out above, are appropriate and proportionate.

6.37 Our aim is to implement guidance which seeks to secure the provision of networks and services which are robust, available, and working well, both in the provision of voice calls and the provision of internet access services generally, ensuring an appropriate level of resilience for consumer services across the UK.

6.38 We have concluded that the measures included in the Guidance for the control plane are appropriate to achieve this aim as, if these measures are not taken by providers, there is an unacceptably high risk of significant loss of connectivity for end users.

6.39 In designing guidance relating to the control plane above, we have drawn upon a number of best practice documents that have been developed by industry over time. Of particular relevance are the standards and guidance that have been prepared by the GSMA[155] and NICC[156].

6.40 The Guidance includes resilience measures we consider to be good practice in that they are featured in several GSMA guidelines documents that are used by providers across the world. The Guidance also includes references to those good practice approaches which should be considered by providers to help ensure that resilience is optimised at the control

[153] European Telecommunications Standards Institute Industry Specification Group Network Functions Virtualisation (ETSI ISG NFV) - https://www.etsi.org/deliver/etsi_gs/NFV-REL/001_099/003/01.01.02_60/gs_NFV-REL003v010102p.pdf

[154] https://kubernetes.io/docs/concepts/scheduling-eviction/assign-pod-node/

[155] The GSMA is a global organisation that represents the interests of mobile operators worldwide. The GSMA works with its members to develop and promote standards that ensure the interoperability and security of mobile networks and services. The GSMA has a number of different committees and working groups that are responsible for developing specific standards. These committees and working groups are made up of experts from mobile operators, vendors, and other stakeholders, and they work together to develop standards that meet the needs of the industry: GSMA, 2023. *About.* https://www.gsma.com/gsmaeurope/about/ [accessed 22 November 2023].

[156] NICC is a technical forum for the UK communications sector that develops interoperability standards for public communications networks and services in the UK. NICC is an independent organisation owned and run by industry members. NICC relies on its members and the wider UK industry to define its work programme and to contribute the resources to develop standards: NICC, 2023. *About NICC.* https://niccstandards.org.uk/about/ [accessed 22 November 2023].

plane aspects of their network, and contains further examples of the mechanisms and frameworks which communications providers could implement in order to ensure they are meeting their security duties.

6.41 For example, the GSMA documents referred to in the Guidance provide guidance and requirements on how to design, operate, and secure mobile network to network interfaces (NNI) and user to network interfaces (UNI)[157] for interoperability, optimal performance, reliability, and security.[158]

6.42 The Guidance also refers to measures on the control plane prepared and published by NICC. These include documents prepared by NICC task groups, including those looking to develop best practice approaches to SIP overload control.[159] The objective of this task group, and the practices it prescribes, are to inform providers on how to improve the resilience and performance of SIP networks in the UK and ensure that SIP-based network services remain available even under overload conditions.[160]

6.43 The Guidance has also been developed with a consideration of recent experience of real-world UK communications provider network failures and outages captured as part of Ofcom's own incident reporting regime.

6.44 We have recorded a number of control plane incidents. One incident led to a provider's customers being unable to register onto the network and led to 3.5 million customer-hours being lost.[161]

6.45 We recorded further control plane incidents at a separate provider, whose whole customer base was subject to short but regular durations of poor service quality (estimated to be approx. 7.8 million customer-hours of poor of experience).

6.46 A further example included an incident at a communications provider, where database replication issues led to 2.8 million customer-hours being lost.

6.47 We have also recorded several different SIP signalling 'overload' incidents in both fixed and mobile networks. Some of these SIP 'overload' incidents specifically impacted end-user devices by disconnecting them and preventing them from re-registering to the SIP voice core. Other SIP overload incidents impacted network interconnections and prevented calls between networks.

---

[157] 'IPXs' are high-performance, high-capacity IP networks that are used to interconnect MNOs, fixed network operators (FNOs), internet service providers (ISPs), and other service providers. IPX networks are separate to the internet and support service level agreements for deterministic quality of service.

[158] For example, GSMA IR.77 contains security requirements underpinning IPX connections and interconnection, and GSMA AA.51 provides an architectural overview of IPX and how component parts of services should be segregated and carried over Interconnects. The same principles apply when providers interconnect directly between themselves instead of via an IPX provider, including in the context of Virtual Network Operators. GSMA, 2007. *Inter-Operator IP Backbone Security Requirements For Service Providers and Inter-operator IP backbone Providers* ; GSMA, 2021. *Guidelines for IPX Provider networks*.

[159] A SIP network is a network that uses the Session Initiation Protocol (SIP) to control the establishment, maintenance, and termination of real-time communication sessions. SIP networks are the basis for many modern communication services, including VoIP, video conferencing, and instant messaging. SIP networks are also used to support emerging services, such as the Internet of Things (IoT) and machine-to-machine (M2M) communication.

[160] NICC, 2023. *ND 1657 SIP- Overload Control*.

[161] The 'user hours lost' figures used in this section are an Ofcom estimate.

6.48 Other types of ‘overload’ incidents include a provider seeing ‘diameter’ overload issue which initially caused significant impacts within their own network. However, these issues spread to another provider via interconnection, affecting their core systems and negatively impacting their own customer base.

6.49 A separate provider experienced an outage of their real-time charging engine due to a lack of failover between core sites. This adversely affected half of their customer base.

6.50 These experiences, and particularly the impact that these have had on end users, demonstrate that the measures included within the guidance are appropriate in order to reduce, or eliminate, some of the resilience problems we have seen in practice. If providers implement the measures included in the guidance, we consider it far more likely that incidents, such as those outlined above, could be avoided or have a less severe impact.

6.51 We should also note that any recommended measures included in the Guidance will need to be considered in the context of any given use case, so may not always be necessary or relevant in all scenarios. It would still be for the provider to assess what aspects of the guidance are relevant to their own set of use cases in order to fulfil their security duties under s105A-D. We consider that this approach allows providers to only implement those of our described measures which are necessary in order to fulfil their security duties under s105A-D in a given instance.

6.52 We therefore consider that the measures set out for the control plane are proportionate as they go no further than is necessary in our view to provide an appropriate level of resilience, including providing flexibility where appropriate.

6.53 We also consider that the proposed measures will not produce adverse effects which are disproportionate to the aim pursued.

6.54 In addition to the proactive engagement mentioned as part of Ofcom’s Incident Reporting function, following network and service outages, Ofcom has undertaken significant engagement with providers to understand how their control plane systems have been set up and operated. These proactive and post-incident engagements have included all of the major UK fixed and mobile operators, plus a reasonable cross section of smaller providers that operate with relatively smaller user bases e.g., alternative network providers. We have also undertaken a detailed public consultation on proposed guidance measures relating to the control plane.

6.55 Our conclusion from these engagements is that most of the design and operational expectations included in the Guidance are already implemented by most of these providers.

6.56 However, the post-incident engagements, where incidents resulted in significant network and service outages, have highlighted examples where we consider providers would benefit from guidance in order to ensure that going forwards, they are clear on how we expect them to meet their resilience-related security duties. Through the Guidance, we therefore seek to clarify our expectations on appropriate and proportionate measures that providers should take in relation to their network design and operational models. In most cases, following incident reviews with Ofcom, providers have implemented appropriate changes to their networks or services to prevent, or minimise, the likelihood of future occurrences.

6.57 Our view, therefore, is that providers who follow the Guidance are unlikely to incur significant additional costs. Indeed, the NICC ND.1657 document on SIP Overload Control,

mentioned above, states that *'the majority of the mitigations mentioned here are low cost and can be implemented using existing features on network devices…'.*[162]

6.58 Therefore, we regard the Guidance measures at the control plane as proportionate given the importance of the control plane and the likely low cost of implementing the proposed measure.

Management Plane Resilience

Consultation proposals

6.59 The management plane is used for configuring, monitoring, and troubleshooting network devices. Examples of its use might include configuration changes, pushing out software updates to network devices, receiving alarms and other telemetry from network equipment and functions, identifying performance bottlenecks, and identifying the sources of outages. This functionality helps to optimise reliability and security on the network.

6.60 The management plane can be implemented 'in-band' over the same physical production network as the user and signalling planes with appropriate segregation, as well as using a dedicated management network, which is separate from the main production network relied on by end users. This is described as 'out-of-band' (OOB) management. This helps to protect the management plane from being affected by issues on the main production network, but also avoids the management plane impacting on the production network.

6.61 The proposed guidance (section 4.4) stated that whilst in-band management is typically more cost effective, we would expect providers to take measures to ensure sufficient segregation of management traffic and production traffic, including mechanisms to ensure management traffic can neither be impacted by or have an impact on the production traffic. As a minimum, we said that we would expect this to include logical separation of management traffic into different VLANs and VPNs/VRFs to limit the potential for problems in one virtual routing or switching domain impacting another.

6.62 The proposed guidance (section 4.4.1) also emphasised the benefits of having an OOB management function available for key network equipment. It enables providers to carry out critical tasks even when the main network goes down. For example, having a dedicated network allows a provider to restore services on multiple and geographically dispersed sites if they fail, meaning that time consuming and labour intensive 'truck rolls' can be avoided, and instances of network downtime can be significantly reduced. It can also help to ensure better security, enable reliable network auditing, and generally help in improving reliability of the network.

6.63 The Public Switched Telephone Network (PSTN) has sometimes been used as a method for OOB access, using analogue lines or ISDN lines, based on the logic that they are often physically separate to the rest of their network. With PSTN switch off, providers will need to consider alternative methods, or risk losing OOB management functionality. Multiple options are available depending on the provider's needs, for example, there are options based on PON[163] and 4G/5G connectivity which could provide this function for some

[162] NICC, 2023. *ND 1657 SIP- Overload Control* p.7.
[163] Passive Optical Network.

operators. We did not prescribe in detail what method of OOB management should be used because the best option for a given provider is likely to vary.

Summary of responses

6.64 Sky said the in-band management measures in the proposed guidance are over-prescriptive. It stated that the logical separation of management traffic may be unnecessary, noting changes being made by providers to management planes as a result of the Security Code of Practice.[164]

6.65 Gamma said that isolation should be further enhanced within the management plane by segmentation (via VLANs or similar technology) into sub-networks that are dedicated to specific platforms. It said this reduces the risk of an incident within the management plane moving laterally across the plane or across network elements under management.[165]

6.66 Several respondents were broadly supportive of Ofcom's proposals for the management plane, with two highlighting how providers will need to consider alternative OOB systems once the PSTN is switched off.[166] SynOptika said the ceasing of the PSTN, and move away from ADSL products, will require extensive work by all operators to create resilient OOB management planes.[167]

6.67 However, there were differing views on the degree of prescription in the proposed guidance in relation to out of band management systems.

6.68 Openreach queried if the proposed guidance provided the flexibility to use more 'manual' approaches for the management plane.[168] Further, it said that the proposed guidance suggested that larger providers should adopt OOB systems for the management plane.

6.69 In contrast, Vorboss said Ofcom should be more prescriptive in relation to the security and resilience of OOB management networks, and SynOptika said a resilient OOB management plane should be a 'requirement'.[169]

6.70 Voxyonder stated that it is important for providers to conduct due diligence if they are procuring connectivity from another provider for their OOB connection, to check that the OOB network is topologically separate to their own to avoid any single or common points of failure, should their network fail.[170]

---

[164] Sky response to the consultation, p.6.
[165] Gamma response to the consultation, p.5.
[166] Ofcom, 2024. *Moving landline phones to digital technology: what you need to know*
[167] SynOptika response to the consultation, p.2.
[168] For example, Openreach (at paragraph 29, p.6 of their response) explains that it utilises both OOB approaches and other approaches to resilience: For Ethernet and Optical services – it uses 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: it uses 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. Openreach consider their 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. Openreach 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.
[169] Vorboss consultation response, p.2; SynOptika consultation response, p.2.
[170] Voxyonder consultation response, p.11.

6.71 Azenby Ltd. highlighted the importance of backup provision for network management centres. It noted that, while not strictly a management plane topic, this should be part of an operator's disaster recovery plans, which should be regularly tested. It believed this should be reflected in the guidance.[171]

Assessment of responses to proposed Management Plane measures and resulting changes to the proposed guidance

6.72 Again, we have decided broadly to maintain our approach to the management plane in the Guidance.

6.73 We note Sky's comment that the proposed guidance was overly-prescriptive, and that the logical separation of management traffic may be unnecessary. The Guidance describes the key concepts which are relevant to resilience-related security compromises, and we consider that the Guidance on management network logical separation is consistent with the Security Code of Practice (particularly measures M11.14-M11.18 and M11.23), which focuses on cyber-type security compromises. We also now refer to the Code of Practice for additional details on measures related to management plane segregation.

6.74 We agree with Gamma's comment on the point of separation/isolation of the management plane into sub-networks for different specific platforms (via VLANs or similar). This was already covered in section 4.4 of the proposed guidance in the last sentence of the second paragraph which stated: *"As a minimum, we expect this to include logical separation of management traffic into different VLANs and VPNs/VRFs to limit the potential for problems in one virtual routing or switching impacting another."* In light of Gamma's feedback, we have modified the last sentence of section 4.4 for clarity to say: "As a minimum, we expect this to include logical separation of management traffic into different sub-networks (e.g. VLANs/VPNs/VRFs) for different network platforms or functions (e.g. types and/or vendors) to limit the potential for problems in one management sub-network to impact another."

6.75 SynOptika are right to highlight that the closure of the PSTN, and reduced use of ADSL, means OOB management based on these technologies will need to be replaced. However, we would note that there are range of different OOB solutions used by providers beyond these legacy technologies.

6.76 We note Openreach's query on whether the proposed guidance provides sufficient flexibility to deploy more manual approaches to the management plane. We have been mindful to avoid specifying the implementation of a particular type of OOB management system. Setting out more precise measures in relation to OOB management would in our view be impractical given the diversity in the size, architecture, and operation of provider networks. We therefore consider that the Guidance does provide sufficient flexibility for providers to adopt their own approaches and have decided not to make any changes to the text included in the proposed guidance.

6.77 However, we would generally expect it to be appropriate for larger providers to have a more scalable OOB system than smaller providers to meet their management needs. For example, in the case of a larger provider, the scale of end-user disruption resulting from not being able to restore services remotely quickly and easily on multiple and geographically dispersed sites would be significant in the absence of a sufficiently scalable OOB

[171] Azenby Ltd. consultation response, p.3.

management solution. This has been demonstrated by the international examples provided in our consultation (4.94-4.98).[172]

6.78 While we have set out what we consider to be best practice at a high level, the Guidance is not the only way for providers to comply with their resilience-related security duties. Therefore, this does not preclude larger providers from using other resilient solutions at the management plane, including more manual approaches if they consider they are appropriate for their needs, although we would expect a provider to be able to explain the solution, approach, or measures they have taken in this regard.

6.79 We agree with Voxyonder's point about the need to conduct due diligence when procuring OOB services to avoid any single or common points of failure. We believe this is a principle that should generally be adopted by providers when making procurement choices across their networks and services. We consider that the type of procurement due diligence scenario described would be consistent with the types of measures that providers should take to identify and reduce the risks of security compromises occurring when using third party suppliers.

6.80 We have added some additional signposting to the opening section of 4.5.3. This is to address a question from Virgin Media 02 on what 'service design requirements and obligations' means. The opening section now directs the reader to 5.1.1.1, where this term is explained.

6.81 In response to Azenby Ltd's comment, we have added text to the Continuity Management section (5.1.1.4) of the guidance.

Decision on resilience measures at the management plane

6.82 We consider that the decisions we have taken in the Guidance on measures at the management plane, as set out above, are appropriate and proportionate.

6.83 Our aim is to implement guidance which seeks to secure the provision of networks and services which are robust, available and working well, both in the provision of voice calls and the provision of internet access services generally, ensuring an appropriate level of resilience for consumer services across the UK.

6.84 We have concluded that the measures we set out in our Guidance for the management plane are appropriate to achieve this aim as, if these measures are not taken by communications providers, there is an unacceptably high risk of significant loss of connectivity for end users.

6.85 In designing the Guidance relating to the management plane, we have taken into account a number of well-established industry standards and guidance documents that have been developed over time, with input from industry. Many different standards organisations

[172] Ofcom 2023, *Resilience guidance consultation and Call for Input on mobile RAN power back up*, p31.

have written about network and IT systems management including: ISO[173], ITIL[174], ETSI[175], ITU[176], ENISA[177], EC-RRG[178], NRIC[179], TMN[180], COBIT[181], etc.

6.86 The EC-RRG Guidance advises that 'Network management plays a vital role in maintaining resilience by providing data on events and alarms in the network, allowing the provider to take corrective actions as required. The appropriate use of statistical data collection is an essential part of network management. Properly designed network management and procedures should mitigate losses due to internal and external events.'[182]

6.87 The Security Code of Practice contains a range of more specific measures related to network management and monitoring.

6.88 There are also examples from outside of the UK, including the US, where networks and services have experienced significant issues as a result of not having OOB management in place or working correctly. We consider these are relevant as the supporting technologies and design of networks in the US are comparable with those used in the UK.

6.89 In October 2021, Meta experienced a global outage, impacting many of its services including WhatsApp, Facebook and Instagram. Although Meta states in a publicly available engineering update that the trigger for the outage was a failure in the system that manages their global backbone network capacity, it also explained that the outage was prolonged by the absence of a workable OOB management function:

'Our primary out-of-band network access was down, so we sent engineers onsite to the data centers to have them debug the issue and restart the systems. But this took time, because these facilities are designed with high levels of physical and system security in mind. They're hard to get into, and once you're inside, the hardware and routers are designed to be difficult to modify even when you have physical access to them'.[183]

6.90 The FCC's review of 2020 T-Mobile incident in the US where an outage lasted 12 hours, referenced above at 4.46, also included observations about the importance of communications providers being able to remotely manage their network to diagnose and

---

[173] International Organization for Standardisation is a non-governmental organisation that develops and publishes international standards for a wide range of products, services, processes, and systems.
[174] The Information Technology Infrastructure Library (ITIL) (discussed further at 5.134).
[175] The European Telecommunications Standards Institute is a standards development organisation that develops standards for information and communication technologies.
[176] The International Telecommunication Union is an international organisation within the United Nations where Member States and business coordinate global telecom networks and services.
[177] European Union Agency for Cybersecurity (ENISA) is the European Union's centre of expertise in cybersecurity.
[178] The Electronic Communications Resilience & Response Group (EC-RRG) is a cross government and telecoms industry forum whose aim is to ensure the telecoms sector remains resilient to threats and risks to services.
[179] The Network Reliability and Interoperability Council is an advisory committee to the Federal Communications Commission (FCC) on telecoms network reliability and interoperability.
[180] The Telecommunication Management Network is a protocol model defined by the International Telecommunication Union (ITU-T) for managing open systems in a communications network.
[181] Control Objectives for Information and related Technology, is a framework for managing information technology (IT) in an organisation. It provides a set of best practices that organisations can use to improve their IT governance, risk management, and compliance.
[182] EC-RRG, 2021. *EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure*. p30. Section 8.2.1
[183] Meta, 2021. *More details about the October 4 outage*. https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/ [accessed 22 November 2023].

remedy outage incidents. Their investigation concluded that T-Mobile's inability to remotely access parts of their network prevented them from diagnosing and fixing problems on their network in a timelier way:

'Had T-Mobile maintained a separate communications channel to enable it to manage the affected router even when they took the suspected link down during troubleshooting, they could have maintained superior visibility into the network and potentially resolved the outage more quickly.'[184]

6.91 The FCC report goes on to say, '*T-Mobile implemented this best practice as a corrective action to prevent a recurrence of this event*'.[185] We note that the best practice they refer to has been in place since at least 2011.[186]

6.92 We note that the FCC reached a similar conclusion in their investigation into a separate nationwide, 37-hour outage in 2018, concerning another large US network, CenturyLink (*now Lumen Technologies*) Inc. As many as 22 million customers across 39 states were affected by the outage, and at least 886 calls to 911 were not delivered.[187] The FCC concluded the outage was caused by an equipment failure catastrophically exacerbated by a network configuration error. However, a key recommendation included in their network outage report was that network administrators should have secondary network monitoring procedures in place for when primary network monitoring procedures are inoperable or insufficient:

'Standard operating procedures for network repair should address cases where normal networking monitoring procedures are inoperable or otherwise unavailable. CenturyLink's network administrators were unable to connect to nodes remotely to locate and diagnose the outage or take corrective action because of node congestion.'[188]

6.93 These experiences, and particularly the impact that these have had on end users, further strengthen our view that the measures included within the guidance are appropriate, and necessary to avoid unacceptably high levels of risk of significantly high loss of connectivity to end users. If providers implement the measures included in the guidance, their ability to identify network issues, and respond in an effective and timely way, will be significantly enhanced, and the risk of incidents, such as those outlined above, would be greatly reduced, or such incidents would have a less severe impact.

6.94 We also consider that the measures set out for the management plane are proportionate as they go no further than is necessary in our view to provide an appropriate level of resilience, including providing flexibility where appropriate.

6.95 In preparing the measures outlined in the management plane guidance, Ofcom has been mindful to avoid specifying what providers should do in detail. For example, we have not sought to prescribe the implementation of a particular type of OOB management system.

---

[184] Federal Communications Commission, 2020. *June 15, 2020 T-Mobile Network Outage Report*. p.17 paragraph 45.
[185] Ibid.
[186] Communications Security, Reliability and Interoperability Council, 2011. *Best Practice 13-10-0409*. https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data [accessed 22 November 2023]. To access data, search 0409 in BP Number search tool.
[187] Federal Communications Commission, 2019. *FCC ISSUES REPORT ON CENTURYLINK NETWORK OUTAGE; Agency Shares Findings and Recommendations to Bolster Network Reliability and Help Prevent Similar Outages*
[188] Federal Communications Commission, 2019. *A Report of the Public Safety and Homeland Security Bureau Federal Communications Commission August 19, 2019.* p.15 paragraph 40

Instead, we recognise that providers should introduce OOB management solutions that are tailored to the nature and scale of their own network. For example, relatively small providers with a limited number of sites may consider they can respond to issues such as infrastructure failures quickly and effectively by taking a manual approach to restoring services (e.g., a van roll to all of their sites within hours). However, with larger providers, with multiple sites, it is likely that such a manual approach would be impractical. We would therefore expect these larger providers to adopt a more scalable OOB system to better meet their management needs. We consider that this approach allows providers to only implement those of our described measures which are necessary to fulfil their security duties under s105A-D in a given instance.

6.96 We also consider that the proposed measures will not produce adverse effects which are disproportionate to the aim pursued.

6.97 Ofcom has undertaken significant engagement with providers to understand what measures they currently take at the management plane. Our conclusion from these engagements is that most of these providers do run some form of OOB management system already, some of which are still based on the PSTN. As the PSTN is set to be de-commissioned over the next few years, we would expect providers to be increasingly focussed on adopting alternative solutions. We have also undertaken a detailed consultation on proposed guidance measures relating to the management plane.

6.98 Our view is that most providers would need to invest in a resilient management plane as a primary requirement to maintaining the availability of their network. As such, our view is that the importance of an OOB system, or any other resilient solution at the management plan, is large enough to justify the cost of implementing a new and appropriate system following the decommissioning of the PSTN. Therefore, we regard the guidance measures at the management plane as proportionate.

‘Communications Provider-managed’ services

Consultation proposals

6.99 The consultation explained that the scope of the proposed guidance extends beyond the underlying infrastructure of providers’ networks and also applies to the services that many providers run over those networks. Some services are consumed directly by end-users, but others operate to support a range of other activities needed to run the network. These are often described as provider managed services.

6.100 The proposed guidance explained that providers would need to give additional consideration to these services when designing and running their network (section 4.5). Of particular importance are voice services, both on fixed and mobile networks. There are several reasons why voice services were singled out in proposed guidance as being ‘a specialised service’.

6.101 Voice services will run over the same network infrastructure as a range of other services (e.g., data traffic for video services and other high bandwidth applications), and due to capacity constraints, there may be occasions when parts of the network become congested. This can lead to a slowdown in network traffic at certain pinch points in the network.

6.102 So that voice services can work effectively, voice traffic needs to pass from user to user in real time to avoid delays that can lead to poor call quality or dropped calls. This risk can be

mitigated by prioritising voice services over other types of service traffic that can cope better with delays.

6.103 Voice service prioritisation can also help ensure compliance with General Condition A3, requiring providers to provide end users with access to emergency services, introduced to ensure the availability of voice services when contacting emergency services.[189]

6.104 The proposed guidance also set an expectation that providers should design, host, and operate critical services (such as 'primary line' voice services) entirely within their own infrastructure, in a manner that does not depend on the functioning of the wider internet. This approach not only reduces risks to the reliability of voice services but can have the additional benefit of reducing cyber threats. The proposed guidance also required that providers make provision for fast and scalable failure detection and failover mechanisms to minimise any negative impact to provider managed services that may result from resilience failures.

6.105 Service operation relates to managing a service through its day-to-day production life. The proposed guidance (section 5.3) set out a number of management requirements that providers should consider to help ensure services run well and any issues are quickly identified. These involve having adequate management tools in place to monitor service events, incidents and problems.

6.106 The proposed guidance (section 5.4) reminded providers that staff competency is key to supporting resilient systems and processes. The proposed guidance explained that care should be taken to ensure staff responsible for key aspects of network design, build, and operations, have adequate training and experience. Staff employed through third parties, such as contactors, should also meet these standards.

Definitions of Communications Provider-managed services

6.107 During the consultation period, Ofcom was contacted by several providers seeking clarification of some definitions that we included in the proposed guidance relating to provider-managed services. We responded by publishing certain clarifications.[190]

Summary of responses

6.108 Several respondents noted that they broadly agreed that the measures in the proposed guidance are appropriate and proportionate. A number of issues were raised that are outlined below.[191]

Service implementation independent of the wider internet

6.109 Several respondents queried certain aspects of the proposed guidance set out in 4.5.1. that related to the provision of voice services. There were two related issues in particular that they sought clarification on:

a) The meaning of the term 'primary-line' voice services at footnote 38 of the proposed guidance; and

[189] Ofcom. *General Conditions of Entitlement.*
[190] The clarification requests , and Ofcom's responses, are set out on the landing page to the consultation.
[191] BT response to the consultation, p.16; Gamma response to the consultation, p.5; Openreach response to the consultation, p.7; Sky response to the consultation, p.6; Three response to the consultation, p.7.

b) The implications of using such a term in the final guidance. [192]

6.110 Respondents explained that the term 'primary-line' is confusing and considered other terms are available, for example those used in the General Conditions.

6.111 Further they argued that the use of the term would have significant impact on the Internet-based VoIP market. Respondents explained that VoIP services relying on the general internet are becoming increasingly popular as users transition away from the PSTN. They argued that end users often choose to acquire a broadband connection from one provider and take their voice services from another provider in an internet based/OTT voice manner.[193] In other cases, established fibre network providers may bundle a voice service into a broadband connection and work with a third-party supplier to provide voice services. Such scenarios are increasingly popular among business-to-business suppliers, especially as home-working is increasingly prevalent. Respondents urged Ofcom to consider more fully the impacts on the market of these aspects of guidance.

Use of the Cloud functionality in providing services

6.112 Some respondents sought clarification on aspects of the proposed guidance that related to the security and resilience of deploying telco cloud.

6.113 Sky noted that it broadly agreed with the proposed guidance in this section. It noted the challenges associated with nascent cloud technologies but stated that these can be practically addressed through learning and development in their environments. It suggested that Ofcom's comments on cloud immaturity with respect to security and resilience should be nuanced, to make clear they represent a moment-in-time snapshot rather than an obstacle to cloud deployment.[194]

6.114 Virgin Media O2 noted there is a use case for moving certain workloads to Cloud or hyperscaler PoPs,[195] which is becoming more commonplace for some providers and is a potential future deployment model for others. It sought clarification from Ofcom that such deployments were not prohibited under the proposed guidance.[196]

6.115 BT noted there appeared to be an inconsistency between the proposed guidance and Net Neutrality guidelines on whether 5G slicing is a specialised service. It explained that the proposed guidance notes "that services built using 5G network slices are expected to be considered 'Specialised Services'", and whilst this may be true of some services, there will also be services outside the net neutrality rules, for instance private networks.[197]

6.116 In relation to Telco Cloud, BT noted that whilst it agreed that 'cloud-native' technologies are still evolving, it did not agree that these technologies cannot yet achieve a high level of resilience, security, scale and throughput and that the cloud model opens up the possibility of new end-to-end architectures that enhance rather than undermine resilience. For example, their network cloud model uses container-based network functions. It urged Ofcom to amend the language in this paragraph to "some" cloud technologies may not be mature enough to achieve a high level of resilience, but not all.

---

[192] CCUK response to the consultation, paragraphs 4-9, p.1; Gamma response to the consultation, p.3; Magrathea response to the consultation p.1.
[193] Over the top.
[194] Sky response to the consultation, p.6.
[195] Points of presence.
[196] Virgin Media 02 response to the consultation, p.22.
[197] BT response to the consultation, p.17.

6.117 [✂] asked if measures for modern/future services (such as cloud or AI-based services) have been considered.[198]

6.118 Azenby Ltd suggested that many vendors do not currently have cloud native implementations.[199]

Other Communications Provider-managed service issues

6.119 BT sought clarity on what was expected in this section of the proposed guidance and whether it was intended to follow the approach Ofcom has already set out in the Net Neutrality guidelines. BT quoted the following from the proposed resilience guidance: *"The types of services and approaches mentioned in this section will typically be implemented with enhanced traffic prioritisation and failover/handover resilience mechanisms. This can only be done for a limited number of services due to limitations of scalability and complexity of these mechanisms, and increased cost often due to sacrificed efficiency".* It noted the Net Neutrality regulations already require that when prioritising traffic for specific services, there is "no significant detriment to the general internet". Therefore, as long as this requirement is met there should be no issue with how many services have enhanced traffic prioritisation.[200]

6.120 Virgin Media O2 sought clarity on the meaning of the words at the end of 4.5.3: "Communications providers must make choices that align with their service design requirements and obligations."[201]

6.121 Three requested that we consider some clarifications:[202]

a) In section 4.5.3, with reference to "the failover mechanisms of the platforms, solutions, and designs should be tested in a representative test environment and optimised under load". It suggested clarifying that "optimised under load" applies to the production environment as in general test environments do not have the capability to generate significant load.
b) In section 4.5.3, with reference to "users may be aware of an impact to service for up to a second or two, but do not need to take any action". It suggested to change this to 1-2 minutes as, depending on the protocol, it may take more than 1-2 seconds to detect failure and execute switch-over, e.g., due to heartbeat timer settings.

6.122 Fibrus noted that Ofcom will be aware of an unresolved issue regarding the porting of telephone numbers from the Openreach network to alternative VoIP providers. It requested clarity from Ofcom as to how it could support industry in meeting its obligations to voice users in this context.[203]

---

[198] [✂] consultation response, p.2.
[199] Azenby Ltd. response to the consultation, p.2.
[200] BT response to the consultation, p.17.
[201] Virgin Media O2 response to the consultation, p.22.
[202] Three response to the consultation, p.7.
[203] Fibrus response to the consultation, p.4.

Assessment of responses to proposed 'service' measures, and decision on the final version of Guidance

6.123 Overall, we have decided to broadly maintain our approach to 'Communications Provider-managed' services in the Guidance, subject to the following changes below which address stakeholder comments.

Service implementation independent of the wider internet

6.124 We appreciate that use of the term 'primary-line' may have caused some confusion. We have therefore decided to remove this term from the Guidance. Instead, we will use the term 'digital landline'. By this we mean fixed voice services aimed at replacing PSTN services, but which use the 'Internet Protocol (IP)' to carry voice traffic.

6.125 We have considered the comments made about how Voice over IP (VoIP) services may be impacted by the guidance.

6.126 In our view, the provision of voice services to end users that run over, are dependent on, or exposed to, the wider public internet gives rise to various risks of malicious and accidental outages and impairments; 'security compromises' in this context. This is because the internet's open nature creates a complex support environment with inherent limitations that may present a number of challenges to providers, these include:

a) the internet lacks a coordinated support structure and standardised cascading service level agreements (SLAs). This makes it difficult for providers to guarantee consistent performance and troubleshoot issues efficiently;

b) while the internet fosters accessibility, it also facilitates accidental disruptions and malicious activity. Accidental routing errors and advertisements can significantly impact service, and sometimes these issues lie outside a provider's direct control, hindering rapid service restoration;

c) distributed Denial-of-Service (DDoS) attacks are a persistent threat, as evidenced by the attacks on OTT VoIP providers in the UK (as highlighted in the Connected Nations 2021 report).[204] These attacks can severely disrupt services, causing significant downtime and customer frustration; and,

d) due to the inherent lack of trust within the internet, providers typically remove differentiated service priority markings from data packets upon entering their networks. This eliminates the ability to prioritise critical services such as voice calls or emergency communications.

6.127 Over recent years, we have seen changes in how people access the emergency services. As mentioned above, in 2023, 41.9 million calls were made to 999/112 in the UK. Of those, 79% of calls were from mobile phones, which is an increase from 74% in 2021.205 However, approximately 15% are still made from a landline.206 So we are mindful of the

[204] Ofcom, 2021. *Connected Nations*, p.63.
[205] DCMS, DHSC, HO, 2023. *999 and 112: the UK's national emergency numbers.* https://www.gov.uk/guidance/999-and-112-the-uks-national-emergency-numbers
[206] DCMS, HO, DHSC, 2023. *999 and 112: the UK's national emergency numbers*. https://www.gov.uk/guidance/999-and-112-the-uks-national-emergency-numbers [accessed 22 November 2023].

importance of ensuring that end users have the ability to make emergency calls via a landline. Take up of digital landlines is likely to become more common as users move away from relying on the PSTN to make calls. As things stand, the PSTN is set to close by 31 January 2027, and every fixed phone line in the UK is expected to move to a fully digital network that uses Internet Protocol (IP) across a fibre-based service.[207] We expect that a subset of emergency calls will continue to be made via digital landlines, and we consider that these should meet a high standard of resilience.

6.128 We maintain our view that is not appropriate for 'critical' voice services, that might include emergency calls, to be run over the open internet, but have considered how we can revise the text in sections 4.5 and 4.5.1. to provide more clarity on our expectations on how 'non-critical' voice services (not carrying emergency calls) can be provided to end users in an appropriately resilient way. We are keen to strike the right balance between ensuring adequate resilience outcomes are achieved while avoiding unnecessary restrictions on the arrangements that providers can use to deliver reliable voice services. After consideration, we recognise that expecting all voice services to be exclusively designed, hosted, and operated within providers' own infrastructure may be overly cautious. It is feasible to provide voice services making use of infrastructure which is also used for internet traffic while maintaining a reasonable standard of resilience. We have therefore revised the wording included in the proposed guidance so that non-critical voice calls are not subject to the same degree of restriction as critical voice calls.

6.129 However, we do expect providers to assess their customers' use of the voice services provided and, where appropriate, provide their customers with information about the availability, reliability, and potential risks associated with the design and operational model of the voice services they provide. We would not generally expect customers of a provider to understand the technical or operational limitations or risks of a provider's voice service unless they are made aware of these limitations. Providing such information in appropriate circumstances will allow customers to make more informed choices and thus help prevent some of the risks outlined above from occurring. We consider that alerting customers to such risks would not impose a cost on providers that is disproportionate to the aims pursued. For example, providers may consider publishing information on a prominent part of their company website alongside a description of the product or service features, or include it within the relevant product literature, and flag this specifically to customers in appropriate circumstances.

Use of the Cloud functionality in providing services

6.130 We note comments made by BT and Sky that although resilience challenges exist in the deployment of Telco cloud, these issues can be addressed, and their view that guidance should reflect the potential for cloud as a growth area. It was not our intention to suggest that challenges with Telco cloud deployment were not manageable. While we do not agree that the proposed guidance needs substantive revision, we have revised the relevant text in the Guidance slightly to more closely pinpoint the areas that we consider of most concern, informed by evidence from Ofcom's Resilience Incident Reporting function.

6.131 We have also noted the suggestion from BT that the text relating to the Net Neutrality rules concerning 5G slicing is potentially confusing. On reflection, we have decided to remove

[207] Ofcom, 2024. *Update on PSTN switch off*.

this text from the Guidance as it appears to have resulted in respondents being less clear about the relationship with the Net Neutrality guidance, which was not our intention.

6.132 More generally, and in response to Virgin Media O2's request, we confirm that there is no intention that the Guidance should stymie progress on Telco cloud.

6.133 In the proposed guidance we explained that, at this time, we considered it too early to prepare resilience measures suitable for Telco cloud. As such, we have not prepared detailed guidance for Telco cloud to the degree we have for more established practices in the architecture, design, and operational models that support networks and services. However, given the nascent nature of these technologies and their deployment, we are keen to highlight that many of the potential risks have not yet been fully resolved, so providers should proceed with due caution. Providers should be mindful of their resilience-related security duties when deploying Telco cloud, even though we have not provided detailed guidance on these areas.

Other Communications Provider-managed service issues

6.134 Regarding BT's comment concerning how many services can have enhanced traffic prioritisation, it appears that BT interpreted our text in section 4.5.2 of the proposed guidance as a 'policy statement' (i.e., to mean a specific limit on the permitted number of services). This was not the intended meaning. Instead, our text was intended to acknowledge that there are practical technical limitations of hardware and configuration scalability and complexity that are the limiting factors. This is not related to Net Neutrality. In order to ensure clarity on this point, we have made minor changes to the text in section 4.5.2.

6.135 We note Virgin Media O2's request for clarity on what the words at the end of 4.5.3 of the proposed guidance mean ('*Communications providers must make choices that align with their service design requirements and obligations')*, and we have added text to refer to section 5.1.1.1 of the Guidance which discusses the process of setting the service level requirements for the services that a provider operates with the aim of ensuring that the design of each service can meet the requirements. The obligations referred to in the text are set out elsewhere in the Guidance, and include obligations under the General Conditions of Entitlement, and in particular General Condition A3 in this context. These "obligations" are referred to a number of times through the Guidance and we do not feel that additional text is needed within this section.

6.136 Regarding Three's request for us to consider some clarifications to section 4.5.3 on 'testing failover mechanisms in a representative test environment and optimised under load', and user awareness of failovers which are automatic but have some user awareness at the service level, we have considered both points and explain our decisions below. Regarding Three's feedback on testing of failover mechanisms of platforms, solutions, and designs in section 4.5.3, we continue to consider that these should be tested in a representative test environment, and that the mechanisms be optimised under load. This view is informed by our incident reporting and investigation function where we have found evidence of a concerning number of network or service outages caused by lack of such testing. We appreciate that it may be difficult to achieve a test environment that is 'representative' while also generating a significant enough load (and overload) to robustly test the resilience mechanisms. However, it remains important to ensure that resilience mechanisms work as expected when they are under load because when significant failures occur in live networks, this often results in overload of various network functions and hardware.

Unexpected or incorrect functioning of resilience mechanisms or design approaches in this context can lead to cascading failures. There are a variety of load-generation approaches to achieve appropriate testing of resilience mechanisms of a given network function or piece of hardware in a test environment. We have therefore not made changes to the proposed version of the guidance in this regard.

6.137 In response to Three's suggestion that in section 4.5.3, the text be revised to say '1-2 minutes' instead of a couple of seconds, we consider that a person faced with a 1–2-minute outage would attempt to take the sort of action which would not be consistent with this category of approach. Instead, we have decided to allow for some small additional flexibility in the description by changing the text to "*users may be aware of an impact to service, typically for up to a few seconds, but do not need to take any action*".

6.138 We note Fibrus's response related to porting of telephone numbers. This is beyond the scope of section 105A-D of the 2003 Act and this Guidance, and it may be better to direct queries to the Office of the Telecoms Adjudicator (OTA2). [208]

Decision on resilience measures for communications providers' managed services

6.139 Our aim is to implement guidance which seeks to secure the provision of networks and services which are robust, available and working well, both in the provision of voice calls and the provision of internet access services generally, ensuring an appropriate level of resilience for consumer services across the UK.

6.140 We have concluded that the measures included in our Guidance for the communications providers' managed services are appropriate to achieve this aim as, if these measures are not taken by providers, there is an unacceptably high risk of significant loss of connectivity for end users.

6.141 In designing the Guidance relating to the provision of providers' managed services above, we have taken into consideration a number of industry standards and guidance documents that have been developed with input from industry over time, and reflected those measures which we consider appropriate for providers to take in order to meet their resilience-related security duties.

6.142 The Guidance refers to 3GPP and GSMA standards that prescribe for the separation of voice and internet traffic on *mobile* networks and devices.[209] The Guidance acknowledges that industry standards for voice and internet traffic separation are less developed for *fixed services* though it does remind readers that there are design approaches that can be used to allow prioritisation and separation to enable consistent quality and experience and protection from malicious attacks. As noted in relation to section 4.2.4 of the Guidance, the requirement that voice interconnections should be separate from the internet is also found in GSMA and NICC standards.[210]

---

[208] https://www.offta.org.uk/

[209] 3GPP specifications are used to develop and deploy mobile networks, such as 2G, 3G, 4G, and 5G: 3GPP, 2023. *About 3GPP*. https://www.3gpp.org/about-us [accessed 23 November 2023].

[210] GSMA, 2007. *Inter-Operator IP Backbone Security Requirements For Service Providers and Inter-operator IP backbone Providers* and NICC, 2009. *ND1643: Guidelines on the minimum security controls for interconnecting communications providers*.

6.143 Given the risks associated with network congestion at various parts of a provider's network, and the reality that voice services will not function reliably if the underlying traffic is subject to loss or delay, we consider it is appropriate that the proposed resilience measures, including voice traffic prioritisation, are included in the Guidance. We consider it particularly important that voice services are prioritised to ensure end users have reliable access to voice calls during emergency situations.

6.144 The measures included in the Guidance are necessary to ensure users can make reliable voice calls. In our opinion, a failure to follow these measures is likely to result in unacceptable, widespread and persistent call failures and degradation in quality. To that extent, the measures should be seen as essential building blocks in the provision of a reliable voice service. Furthermore, it is important to have reliable access to voice calls during emergency situations.[211]

6.145 The Guidance measures offer providers enough flexibility to allow them to take action proportionate to their situation and go no further than is necessary in our view to provide an appropriate level of resilience. For example, while as part of their resilience planning, we expect providers to generally ensure that platforms, solutions, and designs include fast and scalable failure detection and failover mechanisms to minimise impact to services. We understand that there are complexity, scalability, and cost implications to the different failover approaches described, and that it is unlikely to be technically feasible or cost effective to support a "zero service impact" approach for all services or traffic types. The Guidance therefore recognises that providers must make choices that align with their service design requirements and obligations.

6.146 We also consider that the measures will not produce adverse effects which are disproportionate to the aim pursued. The measures outlined are regarded as standard practice among most major providers internationally and are intended to reduce any adverse impacts, including reduced voice service quality. Failure to follow these measures is more likely to result in providers not being able to provide a service at all, or with significant impairments to voice call quality.

[211] We consider it likely that the low frequency of emergency situations will result in 'present bias' and informational asymmetries distorting decision making which ultimately results in consumer harm. It is also likely that commercial incentives would not reflect the significant externalities associated with having access to calls in emergency situations.

7. Processes, Tools and Training

Summary

7.1 This section considers the responses to the consultation's questions regarding the appropriateness and proportionality of the proposed guidance on processes, tools and training.

7.2 We provide a reminder of what measures were included, summarise respondents' views on them and explain our final decisions and why we consider they are appropriate and proportionate.

Consultation proposals

7.3 The proposed guidance set out expectations on a number of aspects relating to the 'operational wrap' around underlying physical and logical deployment (infrastructure) that allows for it to be architected, designed, tested, deployed, and operated in an effective manner and to achieve expected levels of availability. These expectations are summarised below.

Network service and design

7.4 When providers are introducing new services, or making changes to existing ones, the proposed guidance (section 5.1.1) set out a number of management practices that should help to ensure services continue to run smoothly, reduce the likelihood of service failures and, when issues do occur, ensure providers have plans to resume services quickly. The proposed guidance set out that providers should have management measures in place to monitor and configure service levels, capacity, availability, continuity, and supplier management. It also described some of the tools that providers can use to support these management activities.

Network and service transition

7.5 The proposed guidance reminded providers that the deployment of new services, and updates to existing ones, requires careful consideration, planning and testing. Section 5.2 set out a number of management practices that should be considered as part of network and service transition.

7.6 These included having:

a) a robust change management plan;

b) up to date registers to record all assets and how they relate to services;

c) a vigorous testing regime to ensure services work as planned after go-live; and

d) a reliable knowledge management system, so information can be retained and easily retrieved for others within the organisation.

7.7 The proposed guidance advised caution when providers rely on automated management tools to perform these functions. Whilst automatic network configuration can be beneficial, it can also lead to catastrophic network failures if not implemented correctly.

Service operation

7.8 Service operation relates to managing a service through its day-to-day production life. The proposed guidance (section 5.3) set out a number of management requirements that providers should consider to help ensure services run well and any issues are quickly identified. These involve having adequate management tools in place to monitor service events, incidents and problems.

7.9 A similar caution about network automation applies to service operation, as set out at 4.122.

Skills competency training

7.10 The proposed guidance (section 5.4) explained that staff competency is key to supporting resilient systems and processes. The proposed guidance explained that care should be taken to ensure staff responsible for key aspects of network design, build, and operations, have adequate training and experience. Staff employed through third parties, such as contactors, should also meet these standards.

Summary of responses

7.11 Ofcom received responses from Arqiva, BT, Aberdeenshire Council, Openreach, Three, SynOptika and Vorboss noting broad agreement with our approach to the proposed guidance in this area. [212]

Network service and design

7.12 BT and Openreach highlighted concern about the reference to the Security Code of Practice when discussing appropriate tools to implement and use in relation to network and service design, and service transition. Both highlighted that the wording used appeared to classify specific tools that would be considered Network Oversight Functions (NOF) for the purposes of the CoP and stated that this was inappropriate in this context. BT said the Security Code of Practice does not specify which services fall into scope and Openreach argued that the wording could lead to the unintended consequence of expanding the range and definition of NOFs outside of the Security Code of Practice.[213]

Supplier Management

7.13 BT and Openreach raised concerns about setting expectations when selecting supplier hardware, software, or solutions. They suggested the measures were too inflexible to apply to all network components, and testing may not be suitable in every circumstance.[214] Three suggested that greater clarity could be provided in the proposed guidance that selection assessment can be based on evidence of testing provided by the supplier.[215]

Capacity Management

7.14 Openreach said it is not a reasonable expectation that providers can plan and build excess capacity for any eventuality, as this would be disproportionate.[216] BT said that the proposed guidance should be clearer that building capacity is not the only solution when it comes to

[212] Arqiva response to the consultation, p4; BT response to the consultation, p18; Aberdeenshire Council response to the consultation, p2; Openreach response to the consultation, p8; Three response to the consultation p8.
[213] BT response to the consultation, p.18, Openreach response to the consultation, paragraph 44, p.9.
[214] BT response to the consultation, p.18, Openreach response to the consultation, paragraph 43, p9.
[215] Three response to the consultation, p.8.
[216] Openreach response to the consultation, paragraph 42, p.8.

accommodating extreme events, as such investment is likely to be inefficient, and the capacity very likely to remain unused after the event.[217]

7.15 Three suggested a change to the following line of the proposed guidance:

"capacity planning and failover mechanisms should allow for the loss of a core site or peering/interconnect site during the busy hour without resulting in network congestion or overload".

It said *"without resulting in network congestion or overload"* should be removed, as typically the loss of a core site would trigger mass re-registration of devices, which may lead to overload in the remaining core sites. It said networks are typically designed to "smooth out" the peak load, with overload protection / throttling mechanisms to allow full service to resume rapidly.[218]

Change Management

7.16 BT suggested an amendment to one of the questions Ofcom proposed should be considered in the implementation of network and service changes:

"Is the impact of the change understood? E.g., has it been tested in a representative environment at full load?"

BT argued that it is not possible to test at "full load" in a representative environment, as it is by definition 'representative' of all subscribers, and therefore the wording should be changed to:

"Is the impact of the change understood? E.g. "has it been load tested in a representative environment?".[219]

Network Control Plane Monitoring

7.17 BT said whilst it can accurately identify in most cases how many subscribers it expects are impacted during network or service fault, it cannot provide exact numbers for voice customers, and asked for Ofcom's recognition of this in its final guidance.[220]

7.18 Three and [✂] said Ofcom's proposed measures on network control plane monitoring are technically complex and expensive. As a result, Three recommended that we state in the guidance that such measures apply where technically feasible and economically viable.[221]

7.19 Virgin Media O2 sought clarification regarding whether the proposed measures apply not only to external signalling but also to internal signalling. Additionally, they enquired about how the proposed guidance aligns with the existing Security Code of Practice concerning these requirements. It also argued that implementing identical logging and monitoring practices for internal networks, as required for external networks by the Security Code of Practice, would not be appropriate, proportionate, or necessary.[222]

Network User plane monitoring

[217] BT response to the consultation, p.18-19.
[218] Three response to the consultation, p.8.
[219] BT response to the consultation, p.19.
[220] BT response to the consultation, p.19.
[221] Three response to the consultation, p.8; [✂] response to the consultation, p22.
[222] Virgin Media O2 response to the consultation, p.22.

7.20 BT said user-plane monitoring for packet capture and more detailed and forensic analysis may not be used in all parts of providers' networks. It said that, whilst it does give a richer view of capacity planning, it is not realistic or proportionate to expect that this is in place across the whole network.[223]

Skills competency training

7.21 Gamma said Ofcom should consider including within the guidance some examples of suitable frameworks, such as Continuing Professional Development (CPD) schemes operated by appropriate professional institutions.[224]

7.22 Vorboss supported Ofcom's view that staff competency is key to supporting resilient systems but had concerns about the potential for unauthorised personnel to access providers' networks, which it said would constitute a security breach, and highlighted increasing prevalence of physical attacks on telecoms networks. It added that network operators must ensure that they know who is accessing their physical network infrastructure, especially where network operators are sharing physical assets. It said Ofcom should consider more direct intervention in relation to Openreach's 'whereabouts compliance' standards if they are not being effectively enforced.[225]

Assessment of responses to proposed process, tools and training measures, and decision on the final version of Guidance

7.23 Overall, we have decided to broadly maintain our approach to 'Processes, tools and training' in the Guidance, subject to the changes we highlight below based on stakeholder feedback.

Network service and design

7.24 The Guidance is not intended to provide prescriptive examples of Network Oversight Functions. To clarify, our objective is to highlight the areas where appropriate tools would be suitable for providers to meet their resilience-related duties. However, we recognise the wording as drafted in the proposed guidance could lead to confusion and we have removed some references to Network Oversight Functions from the Guidance.

7.25 To avoid the risk of misinterpretation highlighted in the responses, the relevant wording on NOFs has been removed from the Guidance.

Supplier Management

7.26 We consider the reliability and resilience tests included in the proposed guidance are established industry practices. They represent reasonable steps that providers should take when selecting supplier hardware, software, or solutions, but we acknowledge it may not be practical to conduct every test in all circumstances. Our intention in designing guidance is to avoid being overly prescriptive, and we consider it is for providers to assess for themselves what is appropriate and proportionate, depending on the specific circumstances. We have sought to provide greater clarification on this point in this section of the Guidance.

---

[223] BT response to the consultation, p.19.
[224] Gamma response to the consultation, p.5.
[225] Vorboss response to the consultation, p.2.

7.27 We have amended the wording to highlight that these types of tests should be carried out "where appropriate".

Capacity Management

7.28 The intention of the Guidance is not to set an expectation that providers should plan and build excess capacity for any eventuality, but instead that they should take reasonable steps to ensure they are sufficiently prepared to anticipate and adapt to foreseeable increases in traffic which will impact networks and services.

7.29 Our proposed guidance stated that "capacity planning and failover mechanisms should allow for the loss of a core site or peering/interconnect site during the busy hour without resulting in network congestion or overload that would affect the ability to manage the network or significantly affect the operation of the network or service". We recognise that we could provide additional clarity in this example, and in the Guidance we highlight that we expect this during a "typical" busy hour, so that any capacity increases can be benchmarked against previous instances where increasing capacity has been necessary to ensure the network did not face significant disruption, appreciating that there may be certain 'super peak' events that are of a scale where this may not be feasible.

7.30 We also acknowledge that a range of approaches can be taken to maintain reliable services during significant network failures and high signalling load conditions. As we have set out at the start of section 4, the guidance is designed to be flexible, and a provider may choose to comply with their resilience-related security duties by adopting different technical solutions or approaches to those specified in the Guidance in order to meet their security duties.

7.31 We have decided to amend the second bullet point in section 5.1.1.2 to clarify our position on the circumstances where we expect our capacity management measures to apply.

7.32 In response to Three, we accept that in some networks the loss of a core site may result in reattachment of a potentially large number of user-devices, and that the control-plane overload controls may result in phased reattachment to the network with some impact on users' service (as outlined in the Guidance, sections 4.3.1 for network functions and 4.3.2 for CPEs/user-devices). However, applying these controls will minimise overall network and service impacts. We have acknowledged this in the Guidance by adding a footnote to the second bullet point in section 5.1.1.2.

Change Management

7.33 We have decided not to amend the text in the final set of Guidance to align with BT's suggestion in the change management section. For the testing of a given network device or function to be valid, appropriate testing needs to be performed with representative hardware, software, and surrounding environment with the relevant 'load metrics' for that given network device or function. It is often when a system or network function is 'under load' that it is most important to ensure that the resilience mechanisms continue to work correctly, as per the design intent. Ofcom has received incident reports where significant outages have been caused by a failure to adequately test under appropriate conditions representative of a live network, and learnings from these incidents underline the necessity to test at this threshold.

Network control plane monitoring

7.34 In its consultation response, Virgin Media O2 asks for clarification about whether the proposed guidance applies to internal signalling, in addition to the Security Code of Practice

measures which require measures relating to external signalling. To confirm, the Guidance does apply to internal control plane signalling.

7.35 As explained in section 4 of this statement, measures contained in the Security Code of Practice relate primarily to cyber security-related malicious acts or attacks. The purpose of including internal network signal monitoring in the Guidance is for resilience rather than cyber security purposes and is distinct. However, it may be feasible to use common monitoring systems for both purposes.

7.36 As we highlight in section 5.3.1 of the Guidance, monitoring of internal signalling in a resilience context can be used, for instance, to identify service issues and ensure appropriate action can be taken to maintain the correct functioning of the function and the wider network.

7.37 The accurate identification of the number of subscribers/devices impacted during network or service faults also supports accurate and timely decisions regarding notification and reporting of incidents to Ofcom.

7.38 In response to comments about the complexity and costs involved, we are aware that MNOs are rapidly moving towards virtualised 5G-SA capable network functions, increasingly based on 'cloud native' principles, which are built on network functions virtualisation infrastructure.[226] Cloudification of a mobile network provides a more dynamic and flexible underlying network capability to enable MNOs to fully utilise 5G technology capabilities. However, it does add additional complexity to the management and operation of the network as discussed in section 4.5.4 of the proposed guidance. Due to the complexity of the technological innovation, traditional operating models for network monitoring are inadequate for cloud-native networks such as 5G networks - particularly in relation to enhanced mobile services including network slicing.

7.39 For example, providing Service Assurance reporting in relation to Service Level Agreements (SLAs) for a given network service, or the provision of a dynamic slice, requires real-time analytics that cannot be derived solely from monitored ingress and egress points as outlined in the Security Code of Practice. Appropriate checks are needed before creating a new network slice. For example, these checks will require the network functions in the core and across the network to provide information to determine if a subscriber can be accommodated on an existing slice, or whether additional capacity or a new slice is needed. Once the service is provided to the customer, the ability for the network to provide service assurance reporting on whether the service met the SLAs will require data from actively monitored network functions. As a result, MNOs will need a level of Core and RAN monitoring in place for virtualised/cloud-based networks (including 5G-SA) to some degree, either from Network Element managers/performance management systems or dedicated monitoring systems.

7.40 In addition, market developments have led to monitoring innovations. The use of analytics and sophisticated machine learning/artificial intelligence anomaly detection are improving, and 'just in time' traffic capture and tracing may be a way of reducing cost to MNOs. If

[226] Virgin Media O2, 2024. *Virgin Media 02 Unveils the Next Phase of its Mobile Network Evolution, with 5G Standalone Switch On.*

traffic is only captured when it is needed, this will greatly reduce the storage requirements (as highlighted by Three).

7.41 We note BT's comments regarding the challenge of accurately predicting the number of individual voice calls that might have been made during an incident, if the incident had not occurred. We appreciate that there will be a margin of error in predicting individual calls. Therefore, we have amended the wording in the final version of the Guidance to highlight that the identification of customers should be relatively accurate.

7.42 UK MNOs have publicly announced live service launches on virtualised cloud-native mobile core networks, including 5G-SA on some networks, noting that a degree of monitoring of network resources and control plane protocols is inherently necessary in this environment to ensure correct and reliable operation of the network and services. The ability to support enhanced 5G SA services and associated service assurance will also rely on these monitoring capabilities. Therefore, we consider the measures included in the Guidance to be appropriate and proportionate.

7.43 In line with our principles for preparing the Guidance, MNOs have the flexibility to take their own approaches to how these measures are applied. For instance, we recognise that it may be suitable to focus monitoring on network technologies which serve the largest proportions of the customer base.

Network User-Plane Monitoring

7.44 We note BT's comments on packet capture and forensic analysis. To clarify, the Guidance does not cover packet capture or forensic analysis in relation to network user-plane monitoring, and we do not consider these points to be directly relevant to the measures we have proposed.

Skills competency training

7.45 The purpose of the Guidance is to ensure staff (or third parties carrying out functions on behalf on the provider) have the appropriate level of skills, competency, and experience to enable the provider to meet its security duties. It is not necessary for Ofcom to set any expectations on professional development beyond that principle. We will, therefore, not be providing information on professional development in the Guidance, but we welcome any initiatives that providers may choose to take to further staff expertise.

7.46 We recognise that unauthorised access to telecoms networks represents a resilience threat and agree that network operators should ensure that they know who is accessing their physical network infrastructure. However, the issue of whereabouts compliance and its enforcement falls outside the scope of our resilience guidance. The contractual arrangements for provision of Physical Infrastructure Access fall within Openreach's Significant Market Power Conditions, and any activities in relation to whereabouts compliance would need to be considered under that regulatory framework. We note that we understand that Openreach is currently taking steps to improve compliance rates.

Decision on resilience measures for processes, tools and training

7.47 Our aim is to introduce guidance which seeks to secure the provision of networks and services which are robust, available and working well, both in the provision of voice calls and the provision of internet access services generally, ensuring an appropriate level of resilience for consumer services across the UK.

7.48 We have concluded that the measures we set out in the Guidance in relation to processes, tools and training are appropriate to achieve our aim as, if these measures are not taken by providers, there is an unacceptably high risk of significant loss of connectivity for end users.

7.49 In designing the Guidance relating to processes, tools and training, we took into account a number of well-established industry-wide standards and guidance documents that have been developed over time, with input from industry.

7.50 Of particular relevance to these aspects is the Information Technology Infrastructure Library (ITIL).[227] ITIL is a framework designed to standardise the selection, planning, delivery, maintenance and overall lifecycle of IT services within organisations. Aspects of the ITIL framework, which have a particular bearing on the availability of telecoms services, have been used and adapted as a basis to provide a structure that aligns with industry recognised best practice. We consider that the inclusion of measures within the Guidance that match those in the ITIL framework is an appropriate means to ensure that providers can implement delivery across their organisations in a resilient way.

7.51 These aspects of the Guidance have also been developed with a consideration of recent experience of real-world provider network failures and outages captured as part of Ofcom's own incident reporting regime.

7.52 Our analysis of reported incidents reveals that outages which resulted from 'design errors' contributed to the second highest amount of lost customer hours (14 million) in 2022/23, even though they represent relatively few in terms of the volume of incidents reported (ten during this reporting period). 'Design error' incidents are extremely impactful when they do occur.

7.53 Additionally, over the course of the reporting period 2022/23, 20 incidents were reported to Ofcom each with an impact exceeding 1 million user hours of lost service. Of these incidents, the top three had a root cause within 'change control' and 'change management'. This included an incident with an impact that exceeded 10 million user hours of lost service. Furthermore, out of these 20 incidents over the million-user-hour mark, 11 were due to 'change activities' and the 'operation of change'.

7.54 Multiple incidents involving 'improper asset management' led to a total impact of 6.5 million customer-hours lost. These incidents involved assets either being incorrectly labelled as non-service impacting, or not labelled at all. The impact of these incidents was compounded by a lack of suitable processes requiring checking there would be no service impact before carrying out any changes or contacting the network operations team if engineers are unsure.

---

[227] The Information Technology Infrastructure Library (ITIL) is a set of detailed practices for IT service management (ITSM) that focus on aligning IT services with the needs of the business. ITIL was developed in the 1980s by the British government's Central Computer and Telecommunications Agency (CCTA) and has since become the most widely used ITSM framework in the world. Until recently, it was owned and managed by Axelos, a joint venture between Capita and the United Kingdom Cabinet Office. PeopleCert, acquired AXELOS in 2021. PeopleCert, 2023. *The world's most widely used IT Service Management framework.* https://www.peoplecert.org/products/itil-certification-family#:~:text=Developed%20by%20the%20Cabinet%20Office,public%20and%20private%20sectors%20worldwide [accessed 4 December 2023]; PeopleCert, 2021. *PeopleCert announces agreement to acquire AXELOS.* https://peoplecert.org/news-and-announcements/peoplecert-announces-agreement-to-acquire-axelos [accessed 4 December 2023].

7.55 There are also examples from outside of the UK where providers have experienced significant issues that may have been avoided if the practices outlined in the Guidance had been followed. We consider these are relevant as the supporting technologies and design of networks in these countries are comparable with those used in the UK.

7.56 A network provider in Japan (KDDI) experienced major disruption in July 2022 that affected over 30 million people for more than three days. The company's own report explained that KDDI's network failure happened while a core network router was being replaced as part of its regular maintenance.[228] The new router prevented the connection of voice calls and, in trying to fix the problem, the carrier experienced heavy concentrations of traffic in parts of the network, which prolonged the outage.

7.57 We note that KDDI's report identified a number of failings that contributed to the cause and the length of time taken to resolve the incident. These included insufficient work preparation (management rules, confirmation items and the way of approval), congestion control was not considered, and no procedures were in place to recover from a complex congestion situation. We also note that the incident has prompted KDDI to implement a number of measures to prevent a similar event occurring again. These included measures to:

'Review the procedures for work and project approval and Project risk analysis of work scheduled to be performed'; the 'Development of more elaborate tools to detect congestion at VoLTE Nodes and Review and inspection of design for congestion control'; and 'Review of recovery procedures when congestion occurs and Development of tools to recover congestion at VoLTE Nodes'.

7.58 Whilst the Guidance does not include these specific measures, they would fit under the more general measures under 'Network Design and Transition', where among other things, we suggest providers should have plans in place to assess risk, having an adequate testing regime completed and have the tools in place to monitor/diagnose problems before any changes are made to a network.

7.59 On 8 July 2022, one of Canada's largest network providers, Rogers Communications, experienced an outage lasting several hours and affecting around 10 million mobile and internet customers. It was also reported that the outage prevented customers accessing 9-1-1 emergency services.[229] A published update from Rogers Communications just after the incident put the cause of the outage down to a routine maintenance update:

'*We now believe we've narrowed the cause to a network system failure following a maintenance update in our core network, which caused some of our routers to malfunction early Friday morning.'*[230]

[228] Kiddi Corporation, 2022. *The July Communication Failure and Our Response.* https://www.kddi.com/english/important-news/20220729_01/ [accessed 22 November 2023].
[229] Canadian Broadcasting Corporation, 2022. *Hamilton man was unable to call 911 during Rogers outage as sister was dying.* https://www.cbc.ca/news/canada/hamilton/rogers-outage-911-call-1.6516958 [accessed 22 November 2023].
[230] Rogers Communications, 2022. *A Message from Rogers President and CEO*. https://about.rogers.com/news-ideas/a-message-from-rogers-president-and-ceo/ [accessed 22 November 2023].

7.60 The incident prompted Rogers Communications to release a further update pledging to roll out an '*Enhanced Reliability Plan'*, including the commitment to invest $10 billion over 3 years on measures to improve 'oversight and testing'.[231]

7.61 In July 2024, the Canadian regulator published a report on the outage. In its assessment and recommendations to Rogers, it stated that "*diligence in implementing the improved change management processes would be the most effective way to avoid a similar outage from occurring in the future*".[232]

7.62 The FCC's review of the 2020 T-Mobile incident in the US, referenced above at 5.143, again provided lessons for providers on how to adequately prepare for making changes to critical parts of the network. Their investigation concluded that the incident was exacerbated by an underlying software flaw that had likely been present in the T-Mobile network months prior to the date of the outage and could have been identified in a test environment:

7.63 'Network operators and service providers should consider validating upgrades, new procedures and commands in a lab or other test environment that simulates the target network and load prior to the first application in the field. T-Mobile had a latent software error in its network that it failed to identify and address before it had a catastrophic impact. Had T-Mobile validated its IP Multimedia Subsystem registration node software and router integration in a test environment that simulated the relevant network segment, it could have discovered the software flaw and routing misconfiguration before they could impact live calls.'[233]

7.64 The Guidance includes specific measures relating to 'Testing and Validation Management'. Our view is that such testing in controlled environments, ahead of any planned network changes, may reduce the likelihood of events such as those referenced above from occurring.

7.65 These experiences, and particularly the impact that they have had on end users, further strengthen our view that the measures included within the Guidance are appropriate.

7.66 We also consider that the measures set out for the control plane are proportionate as they go no further than is necessary in our view to provide an appropriate level of resilience, including providing flexibility where appropriate.

7.67 As mentioned above, Ofcom has been mindful to avoid prescribing standardised measures that apply uniformly across all use cases and providers. The measures included in the Guidance around change management, training, asset identification and management and life cycle management can all be tailored to be used by providers of all types and sizes. Further, the Guidance has been drafted in a way to ensure providers are still able to judge which measures are needed based on their own risk assessments in any given use case. We consider this approach allows providers to take measures that are proportionate to fulfilling their statutory duties. The inclusion of measures that are tied to widely recognised industry standards, such as those in the ITIL framework, should provide providers with a helpful

---

[231] Rogers Communications, 2022. *A Message from Rogers President and CEO*). https://about.rogers.com/news-ideas/a-message-from-rogers-president-and-ceo-2/ [accessed 22 November 2023].

[232] Canadian Radio-television and Telecommunications Commission, July 2024. *Assessment of Rogers Networks for Resiliency and Reliability Following the 8 July 2022 Outage*

[233] Federal Communications Commission, 2020. *June 15, 2020 T-Mobile Network Outage Report*. p.16 paragraph 45.

steer as to how they can build resilient networks, though still allowing for a high degree of flexibility in decision making.

7.68 We expect the implementation of these measures may have a large impact on reducing the currently observed number of customer hours lost. We also consider the flexibility that the Guidance provides should allow providers to improve their process, tools, or training in a way that efficiently improves resilience. Therefore, we regard these aspects of the Guidance to be proportionate.

7.69 We also consider that the measures will not produce adverse effects which are disproportionate to the aim pursued.

7.70 As mentioned above, Ofcom has undertaken significant engagement with providers to understand how the various aspects above (physical domains, management, and control planes etc) have been designed, implemented and operated. These discussions have been a mix of proactive and post-incident engagements. They inevitably involved enquiries about the processes, skills and training in place at these providers, which are needed to support the various network aspects mentioned above. We have also undertaken a detailed consultation on proposed guidance measures relating to resilience measures for processes, tools and training.

7.71 Our conclusion from these engagements is that most of the operational expectations concerning the processes, skills and training included in the Guidance are already implemented by most of these providers. However, the post-incident engagements, where incidents resulted in significant network and service outages, have highlighted examples where we consider providers would benefit from guidance in order to ensure that going forwards, they are clear on how we expect them to meet their resilience related security duties. Through the Guidance, we seek to clarify our expectations on appropriate and proportionate measures that providers should take in relation to processes, skills and training. In most cases, following incident reviews with Ofcom, providers have implemented appropriate changes to prevent, or minimise, the likelihood of future occurrences.

8. Mobile access network power resilience

Summary

8.1 In this section we discuss work being done following the publication of the Call for Inputs (CFI) in December 2023 on power backup measures on the RAN.

8.2 We also outline our planned next steps.

The purpose of the December CFI

8.3 In December, we explained we would run a CFI on ensuring power resilience at the mobile RAN. We explained there were several reasons why doing this would be helpful:

a) MNOs can, and do, experience energy outages, and the UK's growing use of, and reliance on, mobile communications services means that the consequences of energy outages are increasingly acute;
b) Mobile network provision can vary during power outages. Some cell sites have backup power (lasting minutes to days) but it depends on the MNO in question and the site's location;
c) Our existing estimates suggest the costs associated with providing a minimum level of backup of power (1 hour) at every cell site would be high. It was not possible for us to conclude whether this requirement, or similar, would be a proportionate measure based on the information we had available;
d) While we acknowledge that additional measures are likely to be necessary to address resilience issues at the RAN, it was not clear what measures would be appropriate and proportionate under the current security framework.

8.4 Given this context, we set out the information we did have available and invited stakeholders' input on:

a) what services consumers should be able to expect during a power outage; and
b) what a more cost-effective solution could look like to address potential consumer harm.

8.5 Our aim was to prompt a discussion about what power backup MNOs can, and should, provide for their networks and services. We might then be better informed to implement this in our guidance in the future, and/or work with industry and Government to identify and pursue other ways to address this issue.

The responses received to the CFI

8.6 We received approximately 60 responses to the consultation and CFI. Whilst a number of these provided feedback on the guidance document discussed in the previous sections, most responses touched upon the CFI. These were provided by a wide range of respondents, ranging from MNOs and industry groups to local authorities and members of the public.

8.7 The responses demonstrated a clear interest in the subject of mobile resilience. A number of respondents noted that the challenges were not limited to the telecoms sector and required a cross sector response.

8.8 Respondents provided some very useful views and insights into the types of harms that may result from mains outages at the RAN. For example, responses discussed the importance of 999 access, and the need for local authorities and family members to contact individuals (including vulnerable people).

8.9 Some respondents, representing communications providers, also outlined the practical, technical, and environmental challenges of enhancing the level of power backup in the RAN. For example, the particular challenges in rural areas where infrastructure can be more vulnerable to strong winds, flooding and other types of bad weather and where distances can impact repair response times.

8.10 We have noted all these responses and will consider them further alongside additional analysis we are undertaking to inform our understanding of these issues.

Next steps

8.11 As outlined in the December CFI, the amount of existing power backup within the mobile access networks varies. Some MNOs have a small number of cell sites with days' worth of power backup, often at remote sites or 'hub' cell sites, which other 'child' cell sites rely on. Some, but not all, operators also have battery backup in some form at all of their sites (of a minimum of 10-15 minutes).

8.12 We are keen to better understand the extent of existing power back up in more granular detail. This would help determine what is currently being provided by MNOs, and how it addresses what respondents have told us is necessary to prevent harms during an outage. In particular, it may allow us to more accurately assess whether and where power backup may be required, and what magnitude of costs is likely to be required to meet the estimated level of need.

8.13 We want to work with operators and Government to address several matters including:

a) Collecting up to date information from MNOs on the location of tens of thousands of individual mast sites across the UK and extent of existing power back up available at each of them;
b) understanding how masts at these locations can continue to maintain provision of various mobile services such as voice calls, SMS, data services in the event of an outage, including the extent to which customers can continue to benefit from 999 roaming;
c) Using this data to build a picture on the extent of resilience for mobile services across the UK and in more geographical depth or by rurality;
d) Assessing the extent of the difference between current levels of resilience and potential customer needs during outages, e.g. more vulnerable customers may consider they need to remain in contact with family and friends during an outage not just access to emergency services.
e) Quantifying the magnitude of costs involved in implementing the various power backup solutions that would be necessary to match expected level of resilience.

8.14 This exercise is being informed by information collected from MNOs through Ofcom's 2024 Connected Nations process. In future this analysis could be enhanced by information on

historic power outages to overlay the nature, scale and whereabouts of power outages across the UK.

8.15 We are engaging with MNOs and Ofgem to understand how further collaboration and co-ordination with the energy industry can improve resilience during/to power outages.

8.16 Over the coming months, we plan to undertake further analysis of the information we have gathered above. This analysis should help inform answers to the question of whether additional resilience measures are needed for the mobile RAN. It may include the consideration of a range of solutions, rather than a one size fits all approach. We plan to work with government and industry to identify the most suitable way forward.

A1. Guidance

A1.1 Our guidance is available on the Ofcom website:
Network and Service Resilience Guidance for Communication Providers.