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

Proposal for updated guidance for communications providers on resilience related security duties under the Communications Act 2003.

Consultation

Published 8 December 2023
Closing date for responses: 1 March 2024

Contents

1. Overview....3
2. Background....5
3. The statutory framework....13
4. Ofcom's proposed guidance....16
5. Call for Input: ensuring power resilience in mobile access networks....42

A1. Impact Assessment....58
A2. Ofgem data....61
A3. Responding to this consultation....62
A4. Ofcom's consultation principles....64
A5. Consultation coversheet....65
A6. Consultation questions....66
A7. Proposed Guidance....68

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 them to function.

In this consultation document, we are proposing to update our existing resilience guidance to provide greater clarity on how providers of public electronic communications networks and services (PECN and PECS) can comply with their security duties under a new framework for security and resilience that came into force in October 2022.[1] Ofcom has a duty to seek to ensure that providers comply with these obligations. In this document, we refer to providers of PECN and PECS as "communications providers" (or "CPs").

The proposed guidance, summarised in Section 4, 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 communications providers to consider. These are designed to help achieve our aim of ensuring an appropriate level of resilience for services across the UK.

What we are proposing – in brief

We propose to introduce an updated version of our resilience guidance for CPs, which sets out the measures we expect them to take in relation to the resilience of their networks, as part of their security duties under s105A-D of the Communications Act 2003.2

Measures contained in the proposed guidance are flexible enough to apply to all types of CPs offering communications networks and services in the UK, while also allowing for continued technology evolution.

This includes:

- 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.

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

[2] The overarching obligations on providers of public electronic communications networks and services (PECN and PECS) are to take appropriate and proportionate measures to identify and reduce the risk, and prepare for the occurrence, of security compromises, and for the purpose of preventing adverse effects arising from such compromises, including remedying or mitigating such effects where they arise.

- setting out the processes, tools, and training that should be considered to support the requirements on resilience.

Call for input on power resilience of mobile radio access networks

This document also includes a separate call for input on power backup for mobile radio access networks (RAN) in Section 5. These networks are dependent on electrical power to function, and outages can cause significant and extensive service disruption for customers. At this stage, we have not included measures relating to the provision of additional power backup up at the mobile RAN in the proposed guidance.

Currently, the amount of battery backup across the mobile RAN varies by Mobile Network Operator (MNO), in terms of both the proportion of cell sites that are backed up and for how long.

There has been an increasing focus on mobile network resilience following the winter storms of 2021/22 as well as the migration of landline users from the Public Switched Telephone Network (PSTN) to Voice over Internet Protocol (VoIP) technology, which means that some consumers will become more reliant on mobile networks in the event of a power outage that affects fixed networks.

Ofcom is now exploring what additional measures MNOs could take regarding the extent of power backup provision (such as batteries) at mobile RAN cell sites. We have set out a framework for what may be appropriate and proportionate as part of their security duties under s105A-D of the Communications Act 2003, with a view to considering what could be included in our guidance in the future.

Power resilience at the mobile RAN is a complex issue, and we recognise that this forms part of a wider debate and cross industry challenge which requires longer term work and investment to address. We want to start a discussion about what power backup MNOs can and should provide for their networks and services, with a view to implementing this in our guidance in the future, and/or working with industry and Government to identify and pursue other ways to address this issue.

Next steps

We invite responses to our consultation and call for input by 5pm on Friday 1 March 2024. Details on how to respond to this consultation are set out in Annex 3. We intend to publish our statement on the resilience guidance, and next steps on mobile RAN power resilience, in summer 2024.

2. Background

What is network and service resilience?

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

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

a) Physical threats or shocks such as 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.

2.2 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.

2.3 As reflected in the EC-RRG[3] Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure[4], 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; and
d) Business continuity planning and disaster recovery; and
e) Appropriate review processes of previous incidents.

Ensuring appropriate network resilience has never been more important

Consumers and businesses are heavily reliant on these networks and services

2.4 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.[5]

[3] 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.
[4] Electronic Communications Resilience & Response Group, 2021. *Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure*.
[5] Ofcom, 2023. *Communications Market Report 2023*.

2.5 People now access a wide and increasing range of online services across public electronic communications networks and services. This includes gaming, banking, remote working, e-commerce, video-on demand/streaming, as well as government services.

2.6 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.[6] [7] 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.

2.7 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.[8] These figures highlight how these remain important methods of communication even as new technology is adopted.

2.8 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.[9] In addition, online gaming is now played by 38% of adults and 57% of children.[10]

2.9 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 people (90%) said they had made an online shopping purchase in the last 12 months.[11] [12] 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.[13]

2.10 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. Ofcom estimates this market generated revenues of £7.0bn to £7.5bn in 2022.[14] 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.

2.11 Both mobile and fixed networks play a critical role in the event of an emergency. 35 million 999/112 calls were made in 2021, of which 74% were from a mobile and 26% from a landline.[15] In March 2023, the UK Government launched its Emergency Alert service, which

---

[6] 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.'
[7] Ofcom, 2023.*Online Nation 2023*, p12.
[8] Ofcom, 2023. Communications Market Report 2023
[9] Broadcast TV: Barb 28-day consolidated, TV sets only. Subscription video-on-demand: Barb Establishment Survey Q1 2019 and Q1 2023.
[10] Ofcom, 2023. *Online Nation 2023.*
[11] Financial Conduct Authority, 2023. *Financial Lives 2022*
[12] DESNZ, 2023. *DESNZ Public Attitudes Tracker: Consumer Issues Spring 2023*
[13] UK Parliament, 2022. *The impact of remote and hybrid working on workers and organisations.*
[14] Ofcom, 2023. *Cloud services market study – Final Report.*
[15] 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].

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.

2.12 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.[16]

Technology innovations can create opportunities but also pose new risks

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

2.14 5G coverage continues to advance, with 85% of premises being able to get a 5G signal outdoors from at least one MNO and 5G data traffic rose from 3% in 2021 to 9% in 2022.[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 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.[18]

2.15 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 19 million, with MNOs' IoT traffic growing by 20% over the last year.[19]

2.16 In recent months, 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.

2.17 As uptake of new services increase, and technological innovation continues, it is important for communications 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.

---

[16] BBC News, 2023. *Optus outage: Millions affected by Australian network failure.* https://www.bbc.co.uk/news/world-australia-67340901 [accessed 22 November 2023].
[17] Ofcom, 2023. *Connected Nations 2023 Summer Update*. https://www.ofcom.org.uk/research-and-data/multi-sector-research/infrastructure-research/summer-2023 [accessed 22 November 2023].)
[18] Ofcom, 2023. '3*G and 2G switch-off*. https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/2g-and-3g-switch-off [accessed 22 November 2023].
[19] Ofcom, 2022. *Connected Nations 2022*. p26-48. Section 3

2.18 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] Last year, 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]

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

Climate change is leading to more uncertain and severe weather conditions

2.20 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]

2.21 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]

2.22 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.

2.23 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]

2.24 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.

2.25 Due to interdependencies in the utilities sector, an outage in one sector can have a knock-on effect in another. In the case of Storm Arwen, the volume and scale of power outages highlighted the extent of the interdependencies between the energy and communications sectors and the need to improve resilience.

---

[20] The Government have 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*. p8-9

[23] Ibid. p5

[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

2.26 The impact on customers is particularly severe in extended power outages where mobile and fixed line services are both unavailable, and where the length of the outage exceeds any power backup solutions in place within telecoms networks. This can leave customers without any means to communicate, including for calls to the emergency services, until power is restored.

2.27 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.

2.28 Following Storm Arwen, the Electronic Communications Resilience & Response Group (EC-RRG) developed 12 key actions to improve the sector's response and resilience to similar severe storms in future. This included exploring the costs and challenges of making the mobile network more resilient to power outages.[26] We discuss the issue of mobile network power resilience in more detail in Section 5.

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

2.29 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).[27] It has since been adopted into numerous critical areas such as within the National Cyber Strategy and the Integrated Defence Review.[28] [29]

2.30 This focus has 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.[30] This is designed to strengthen the strategic approach that underpins the UK's resilience to all civil contingency risks. Over the coming years the UK Government plans will build upon existing resilience standards to create common but flexible resilience frameworks across CNI sectors, as well as focusing on the assurance of CNI preparedness.

2.31 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.

2.32 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

[26] Electronic Communications Resilience & Response Group (EC-RRG), 2022. *2021/2022 Severe Storms Post-Incident Report.* p6
[27] 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].
[28] HMG, CO, 2022. *National Cyber Strategy 2022*
[29] HMG, 2023. *Integrated Review Refresh 2023*
[30] HMG, 2022. *The UK Government Resilience Framework*

challenges and impacts of climate change.[31] Ofwat has announced that it will accelerate potentially £350 million worth of investment in water resilience schemes.[32]

2.33 Internationally, regulatory requirements for the installation of backup power in mobile networks have been introduced in countries including Norway, Sweden, and Finland. The backup duration varies across these locations but range from at least one hour to up to six hours.

2.34 In addition, the Australian Government has introduced a public finding funding programme to improve the resilience of the country's mobile infrastructure in regional Australia, in response to increasingly severe climate emergencies, such as the 2019-2020 bushfire season. [33]

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 providers of communications 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 the following section.

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 proposed guidance for communications 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.[34] 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 2022, Ofcom received 1,281 reports based on incidents that met the reporting thresholds set out in that guidance. This represented an increase on the 761 reports we received in 2021.

2.37 From the reported incidents, we can track trends in the resilience issues being experienced by communications 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.[35]

2.39 Where incidents have a particularly significant effect on the operation of the network or service, we engage with communications providers to establish the cause, how the issue was

---

[31] Network Rail, 2023. *England & Wales Strategic Business Plan Control Period 7.* p11
[32] Ofwat, 2023. *Accelerated infrastructure delivery project: final decisions.* p4
[33] Australian Government, *Mobile Network Hardening Program.* https://www.infrastructure.gov.au/media-communications-arts/phone/mobile-network-hardening-program [accessed 22 November 2023]
[34] 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*
[35] Ofcom, 2022. *Connected Nations 2022*. p49-59. Section 4

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 communications provider to address our concerns and have seen a reduction in both the number and impact of these events with them.

2.40 Incident reporting also enables Ofcom to better understand what is failing in communications 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 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 providers are critical both to individual consumers and the wider economy.

2.42 Ofcom's principal duty is to further the interests of citizens in relation to communications matters and the interests of consumers in relevant markets.[36] As part of this, we must also have regard to the desirability of ensuring the security and availability of public electronic communications networks and public electronic communications services.[37]

2.43 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) occurring. They must also take such measures to prepare for the occurrence of security compromises, again including Resilience Incidents.

2.44 With this in mind, given the benefits and importance of digital connectivity, and as the availability, functionality, and performance of telecoms networks and services are critical to both individual consumers and the wider economy, 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. 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, reviewed current practices and many industry guidelines, we consider that there are a number of measures which communications providers can and should be taking in order to mitigate the risks of resilience incidents to meet their statutory obligations and help ensure the robustness of their networks and services. Implementation

[36] Communications Act 2003 s3(1)
[37] Communications Act 2003 s3(4)(ea)

of the measures we propose to include in our guidance should help achieve the aim of ensuring an appropriate level of resilience for consumer services across the UK.

3. The statutory framework

Summary

3.1 We use this section to outline the statutory framework that underpins the resilience related security duties imposed on providers of public electronic communications networks and services. 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 public electronic communications networks and services came into force in October 2022. This framework is set out in sections 105A-Z of the Communications Act 2003 and strengthened the existing security duties imposed on providers of public electronic communications networks and services.

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*"[38].

3.6 "Security compromise" therefore includes both "cyber-type" compromises such as those caused by hackers, and other impacts on the resilience of public electronic communications networks and services, 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 proposed 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

[38] Communications Act 2003 s105(2)(a) and (d)

came into force on 1 October 2022, and require communications providers to take specified security measures to meet 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 by s105A and 105C. They require communications providers to take specified security 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[39].

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 of the Act. In exercise of these powers, the Secretary of State issued the Security Code of Practice[40] setting out guidance for communications providers with relevant turnover in the relevant period of more than or equal to £50m. The Security Code of Practice gives guidance on measures which is mainly related to cyber-type security compromises.

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

Ofcom's Duties and Guidance

3.11 Under the Communications Act 2003, 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.[41] 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.[42] In the performance of our duties, we must also have regard (among other things) to the desirability of ensuring the security and availability of public electronic communications networks and public electronic communications services.[43]

3.12 Ofcom must also act in accordance with the six requirements at section 4 of the Communications Act 2003, 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. [44] We have taken account of these duties in formulating our approach and the proposed guidance set out in this consultation.

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

[39] The Electronic Communications (Security Measures) Regulations 2022 (SI933)
[40] DSIT (formerly DCMS), 2022. *Telecommunications Security Code of Practice*.
[41] Communications Act 2003 s3(1)
[42] Communications Act 2003 s3()2(b)
[43] Communications Act 2003 s3(4)(ea)
[44] Communications Act 2003 S4(2), 4(5) and 4(6)

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[45]. We published a General Statement of Policy under section 105Y of the Communications Act 2003 in December 2022.[46]

3.15 At the same time, in December 2022, Ofcom also issued updated Guidance on the resilience requirements imposed by, or under, sections 105A to D of the Communications Act 2003, ("the 2022 Guidance"), in the exercise of our powers under s1(3) and s105Y of the 2003 Act. The 2022 Guidance replaced resilience guidance relating to the previous framework dating from 2017[47]. The plan is for the 2022 Guidance to be superseded by the proposed guidance outlined in the next section.

General Conditions of Entitlement

3.16 PECN/PECS providers are separately required to comply with the General Conditions of Entitlement[48], and in particular, General Condition A3. This General Condition aims to ensure the fullest possible availability of public electronic communications services 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 proposed guidance, outlined in the next section, does not give specific guidance on the General Conditions, but it acknowledges those obligations where doing so provides clarity. [49]

[45] Our powers to assess compliance with the security duties (s105N-R) and powers of enforcement of security duties (s105S-V)

[46] Ofcom. *General statement of policy under section 105Y of the Communications Act 2003*

[47] Ofcom, 2017. *Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003*.

[48] Ofcom, 2023. *General Conditions of Entitlement (Unofficial Consolidated Version).*

[49] Ofcom, *General statement of policy under section 105Y of the Communications Act 2003*

4.Ofcom's proposed guidance

Summary

4.1 We use this section to outline our proposal to introduce an updated version of our current resilience guidance ('*proposed guidance'*). We explain that the proposed guidance should help communications providers better understand and meet their existing resilience duties under section 105A to D, ensuring networks and services are better prepared to deal with the threats and risks outlined in previous sections. We then go on to summarise the main components of the guidance and explain why we have included the proposed measures in the guidance.

Why we are updating the Guidance

4.2 Ofcom has already published several iterations of resilience guidance, the most recent in 2022 ('*the 2022 Guidance'*)[50]. Guidance has the benefit of contributing to effective regulation by improving transparency and understanding. One of Ofcom's regulatory principles is that Ofcom will regulate in a transparent manner.[51] Guidance can serve as a useful means of achieving this principle and to increasing understanding of Ofcom's policy objectives and approach to regulation. We consider that an updated and more detailed version of the 2022 Guidance is necessary for several reasons.

4.3 Industry has signalled that they would like more guidance on how communications providers can demonstrate compliance with the existing network resilience requirements.[52] We also explained, when we published the 2022 Guidance, that we would review and update that guidance at an appropriate time.[53]

4.4 Further, and as explained in our background section above, our proposals 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.

Use of the Guidance/Enforcement

4.5 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.

---

[50] Ofcom, 2022. *Statement: General policy on ensuring compliance with security duties*

[51] Ofcom, 2022. *Policies and Guidelines.* https://www.ofcom.org.uk/about-ofcom/policies-and-guidelines [accessed 22 November 2023].

[52] For example, Ofcom, 2022. *Statement: General policy on ensuring compliance with security duties.* p24. See paragraph 2.90, p24 (summary of consultation responses). *VMO2 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".*

[53] Ibid, paragraph 2.93, p24

b) a power to direct communications providers to explain any failure to act in according with a code of practice under section 105I of the 2003 Act – see sub-section titled "Power to direct providers to explain any failure to act in accordance with a code of practice (section 105I)" in section 3 of the Ofcom procedural guidance.
c) 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.
d) enforcement powers under sections 105S to 105V of the 2003 Act – see section 6 of the Ofcom procedural guidance.

4.6 As with the 2022 Guidance, we will use the proposed guidance as a practical reference both;

- in information gathering and monitoring of network and service resilience when engaging with communications providers and the wider industry; and
- as a starting point for considering compliance as part of any enforcement activities in relation to resilience issues.

4.7 The proposed guidance is not the only way for communications providers to comply with their resilience-related security duties under s105A-D and is not binding. A communications provider may choose to comply with their resilience-related security duties by adopting different technical solutions or approaches to those specified in the proposed guidance.

4.8 Nevertheless, the proposed guidance is intended to set out the general approach which we would normally expect to take in investigating compliance with s105A-D as appropriate. Where a communications provider has taken a different approach to that set out in the proposed guidance, we would expect them to be able to explain their reasons for doing so.

4.9 While the publication of any updated guidance is intended to improve transparency and understanding of Ofcom's expectations around the relevant resilience-related security duties, our view is that communications providers should already be taking measures in order to comply with their resilience related security duties, and 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.[54]

Ofcom's approach to preparing the proposed guidance

4.10 As explained above at 3.1-3.10, our proposed guidance sets out the measures to be taken by communications providers in accordance with their duties under sections 105A-D to take such measures as are appropriate and proportionate to identify, reduce, prevent, and remedy events that may negatively impact the "availability, performance, or functionality" of their networks and services.

4.11 Ofcom's approach to preparing the proposed guidance has been to consider the established best practice in the telecommunications sector which represents, at a minimum, the appropriate and proportionate measures we would expect communications providers to take to comply with their duties. This should help achieve the overall objectives of s105A-D

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

which are to identify, respond to, and prepare for, the occurrence of security compromises – and more specifically in this case, resilience incidents.

4.12 We consider the measures proposed to be the baseline. Communications providers can of course take additional measures to further improve the resilience of their networks and services, and we would encourage them to do so.

4.13 The preparation of the proposed guidance has been informed by:

a) examining existing resilience practices at a wide range of communications providers in the UK and elsewhere;
b) engagement with 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;
c) reviewing published standards that have been developed over many years with input from industry;
d) considering any lessons learned from investigations or reviews into resilience related outages in other comparable countries; and
e) referring to evidence collected as part of Ofcom's own incident reporting regime.

4.14 Close scrutiny of incidents noted by way of points d) and e) above often highlight areas where, in our view, the resilience of networks and services could be improved and where in the architecture of networks failures are happening.

4.15 In preparing our proposed guidance, we have not set out specific measures in relation to every possible use case, which would in our view, be impractical. We have instead included measures setting out a range of more high-level good practices in the architecture, design, and operational models that underpin communications networks and services, and which have broad application.

4.16 In considering best practice in the context of our proposed guidance, we recognise that sections 105A-D apply to communications providers of all sizes. Consequently, the guidance we are proposing in this consultation is intended to be flexible enough to apply to all types of networks and services. It is also intended to be future proofed so it should remain relevant as networks develop and new technologies emerge.

4.17 It is for communications providers in the first instance to assess for themselves (taking this guidance into account) the measures which are appropriate and proportionate in their own particular cases. Clearly, what is appropriate and proportionate will depend on the particular circumstances of the communications provider and to the extent that in any given case the measures that would be appropriate and proportionate for a large provider to take to protect resilience may be different to those appropriate for a smaller company, we would expect to take this into account when applying our proposed guidance.

4.18 We summarise below the key measures set out in our proposed guidance, and explain why we consider these measures are appropriate and proportionate for the purposes of meeting the requirements of sections 105A to D. We summarise our approach to impact assessments, including our equality impact assessment, in annex 1.

4.19 We would welcome views from stakeholders on the inclusion of these measures in the proposed guidance and have posed several questions below.

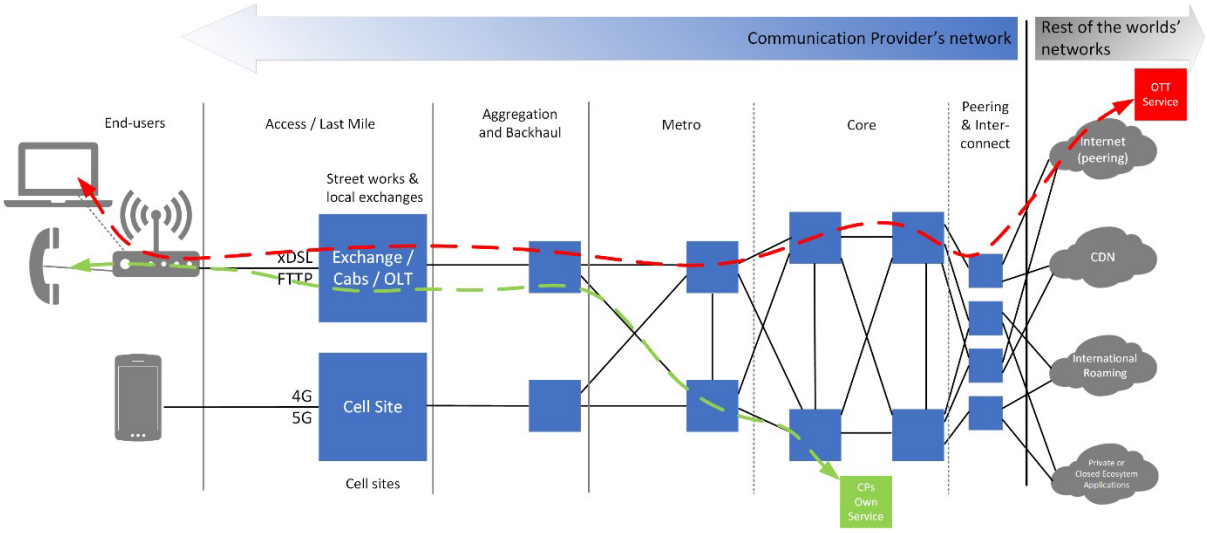
4.20 The full detail of the proposed guidance can be found at annex 7.

Network Infrastructure Domains

4.21 The first part of the proposed guidance focuses on the key physical infrastructure segments or domains that typically form part of a communications provider's network. The network infrastructure within a communications provider's network (*see figure 1 below)* can usually be broken down into the following domains:

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

Figure 1: Typical Communications Provider Network Infrastructure Domains



4.22 In the rest of this section, we briefly discuss the main risks and vulnerabilities that can undermine resilience at each of these domains and then summarise what steps we would expect communications providers to take to address these issues. We also explain why we regard these measures as appropriate and proportionate.

Access / Last Mile

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

4.24 The proposed guidance (section 4.2.1) sets out measures that we expect communications providers to take to mitigate against these risks. These are mostly concerned with communications 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 expect communications 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.

4.25 We note 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 explain that communications providers should provide cabinets (fixed) or mobile base stations with a connection to an additional parent site.

4.26 Further, we explain that we would expect that 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.

4.27 A further key risk at the access level, set out in our proposed guidance, is electrical power backup for active cabinets in fixed networks and walk-in cabins ('active cabinets'). There are a range of technologies 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 communications provider and the customer. Some cabinets rely on electrical power from the grid and cannot function without it. These 'active cabinets'[55] are at risk from localised power outages, which could result in customers losing broadband connectivity until power is restored. We consider that communications providers should maintain a normal level of service in the event of a local power outage. We propose therefore that where communications providers have active cabinets in place, and are not planning to replace or discontinue these within a period of 3-5 years from the date when the proposed guidance is finalised, they should have adequate power backup to ensure they maintain services of at least 4 hours in the event of a power outage at those cabinets.

Aggregation / Backhaul

4.28 The backhaul domain of a communications 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.

4.29 The proposed guidance (section 4.2.2) explains 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 highlights 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 communications 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.

4.30 The introduction of these types of resilience measures can be costly and communications providers may need to prioritise where they deploy these resources to have the most impact. The proposed guidance sets out a number of measures which communications providers can implement to improve resilience. The proposed guidance also outlines the factors which communications providers should consider when deciding where best to deploy these resources. In particular, the proposed guidance advises communications providers to consider Ofcom's 'user hours lost' reporting threshold when deciding on which

[55] 'Active' broadband street cabinets contain electronic equipment that helps to amplify and convert the signals carried by the fibre optic cables. There are also 'passive' broadband cabinets – these do not contain electronic equipment. Instead, they simply splice together lengths of fibre optic cable.

sites to prioritise resilience measures, as this sets out our view of the level at which service impacts are likely to be significant; see section 5 of Ofcom's Procedural Guidance.[56] This approach should provide communications providers with an established method to target resilience measures at parts of the aggregation domain where the largest number of end users will be at risk and therefore where resilience measures offer the most protection.

Core / Metro

4.31 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 communications provider's most critical network and service functions and are typically built to the highest standards of resilience practically and economically possible.

4.32 The proposed guidance (section 4.2.3) outlines a number of measures that communications 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. Communications providers are also 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.

4.33 The proposed guidance explains 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. Communications providers are also advised to consider the location of core sites so that areas with likely geological hazards (e.g., flooding) or patterns of extreme weather, can be avoided where possible.

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

Peering and Interconnect

4.35 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.

4.36 The proposed guidance (section 4.2.4) explains 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 document outlines a number of

[56] Ofcom. *General statement of policy under section 105Y of the Communications Act 2003.* p22-35. Section 5, 'Reporting security compromises'

measures that we expect communications providers to take to ensure that resilience at the peering and interconnect domain remains robust. This includes use of multiple geographically separate paths and third-party networks with appropriate capacity to ensure services run well even when one or more links fail. We further explain that communications providers should also consider physical and logical routes connecting networks beyond the UK, including sub-sea cables.

Why we consider these measures in the network infrastructure domains are appropriate and proportionate.

4.37 We explain above that 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.

4.38 We consider that the measures we set out in our proposed guidance for network infrastructure domains 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. In designing our proposed guidance relating to the physical infrastructure domains above 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.

4.39 Of particular relevance to the network infrastructure domains of a network is the existing EC-RRG Resilience Guidance ('*EC-RRG Guidance*').[57] 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.

4.40 The proposed guidance makes clear that we expect communications 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 proposed 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 best practice, but represent the minimum set of measures which we would expect communications providers to take in order to meet their resilience related security duties.

4.41 The EC-RRG Guidance advises communications providers to assess the risks and invest, where practical, in duplicate or triplicate backups for their equipment ('redundancy') and in diverse transmission routings.[58] Further, it recommends that communications 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.[59] We consider that the measures we propose, relating to the physical network domains, are already recognised within established industry standards as being appropriate

[57] 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]

[58] EC-RRG, 2021. *EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure*. p13. Section 7.1.5

[59] Ibid. p19-20. Section 8.1.1.5

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 proposed guidance.

4.42 The proposed guidance relating to the physical infrastructure domains has also been developed with a consideration of recent experience of real-world communications 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.

4.43 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.

4.44 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 communications providers generated a loss of almost 15 million customer hours, across 3 days.

4.45 There are also examples from outside of the UK, including the US, where communications providers have experienced significant issues that may have been avoided if the practices outlined in the proposed 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.

4.46 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.[60] 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 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.*[61]

[60] Federal Communications Commission, 2020. *FCC ISSUES STAFF REPORT ON T-MOBILE OUTAGE Investigation Identifies Measures to Prevent Similar Outages in the Future*

[61] Federal Communications Commission, 2020. *June 15, 2020 T-Mobile Network Outage Report*. p16 para 45.

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.

4.47 These experiences, and particularly the impact that these have had on end users, further strengthens our view that the requirements included within the proposed guidance are appropriate.

4.48 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.

4.49 In preparing the detail of the proposed guidance, Ofcom has been mindful to avoid overprescribing how communications providers design, build, and operate their networks. Instead, we have sought to ensure that communications providers are able to refer to the proposed guidance measures to help them assess what steps are necessary, based on the circumstances of any given use case. For example, while we expect communications providers to protect onward traffic flows from aggregation sites towards the Core/Metro, we do not necessarily expect communications 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 and active cabinets, where we suggest minimum power back up time periods. We explain this point further below at 4.55.

4.50 We consider that this general approach allows communications providers to only implement those of our described measures which are necessary to fulfil their security duties under s105A-D in a given instance. To assist communications 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 communications 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.

4.51 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.

4.52 Over the last two years, Ofcom has undertaken significant engagement with communications 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 proposed guidance are already implemented by most of these communications providers. As such, our view is that communications providers who follow this guidance are unlikely to incur significant additional costs.

4.53 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[62].

4.54 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 communications 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.

Power at active fixed cabinets and core sites

4.55 We consider communications providers need to factor in minimum 'power backup' time periods on active cabinets and at core network sites. We consider it is appropriate and proportionate to provide more specificity on these measures regardless of size of the communications provider.

4.56 We have concerns about the nature and scale of harms that might result from local power outages impacting active cabinets. We are mindful that active cabinets can typically serve up to a thousand premises, and these could lose broadband connectivity during an outage.[63] Losing connectivity can cause significant harm to individuals, including that caused from a loss of access to emergency calling.[64] We therefore consider it necessary for communications providers to ensure that active cabinets can function for a reasonable amount of time during a power outage to help avoid these harms. In considering what would represent a reasonable time period, we understand from our engagement with industry, including alternative networks, that having 4 hour battery backup is a typical practice when installing new active cabinets to support technologies such as Fibre to the Premise. As such, our view is that this would appear to be an appropriate level of backup.

4.57 We consider that a 4-hour power backup in active cabinets would ensure that customers would be protected from the harms that would likely result from short term power outages. However, we are aware that some communications providers may not currently have any power backup in place within their active cabinets. We are also aware that some communications providers are likely to replace or discontinue their existing broadband infrastructure over the coming years. As such, we consider it would be unlikely to be proportionate for us to expect that these battery backup measures should apply where active cabinets are likely to be replaced in the next 3-5 years. Our view is that it may not be proportionate to expect communications providers to make large scale changes to legacy hardware that is set to be replaced or discontinued in the near future.

---

[62] 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.

[63] A recent press release from Xantaro (*who state that they are a major supplier of services and equipment for UK telecom providers including GoFibre and Upp Network)* explains that their new street cabinet solutions can provide connectivity to up 8,000 homes. We note that the press release also includes the claim that the cabinet can obtain 3-4 hours of battery backup: Xantaro, 2023. *Xantaro launches new street cabinet solution for altnets.* https://www.xantaro.net/co-uk/xantaro-launches-new-street-cabinet-solution-for-altnets/ [accessed 22 November 2023]

[64] At present, most outgoing fixed call are made via the Public Switched Telephone Network (PSTN). This relies on a separate power source to that used in customer premises and less likely to be impacted by local power outages. However, the PSTN is set to be switched off by 2025, when customers will be increasingly reliant on their broadband connection to make an outgoing fixed calls, including those to the emergency services.

4.58 When considering power backup measures at core sites, we are mindful of the scale of harm to end users that may result if power is lost and not restored for any period of time. As explained at 4.34, the loss of a core site has the potential to impact millions of end users, so we consider it is appropriate to implement measures to ensure the continued maintenance of operations in the event of power loss at the grid. The Electricity System Restoration Standard requires the Electricity System Operator (National Grid ESO) to have sufficient capability and arrangements in place to restore 100% of Great Britain's electricity demand within 5 days.[65] We therefore think it is appropriate to expect communications providers to be able to provide power backup at core sites for up to 5 days, as a minimum, to cover this gap. We also understand, from our engagement with communications providers, including alternative networks, that having arrangements in place to ensure power backup at core sites for up to 5 days is a typical practice. As such, our view is that communications providers who follow these power backup measures at the core are unlikely to incur significant additional costs.

Question 1: Do you consider the measures in the proposed guidance relating to the resilience of the physical infrastructure domains to be appropriate and proportionate?

Control plane resilience

4.59 In networking terminology, a plane is an abstract conception of 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 concepts below.

4.60 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.[66] 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.

4.61 The proposed guidance explains (section 4.3) that communications providers should take extra care to ensure extreme reliability/resilience in the design of the network control plane(s). We would expect communications 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. Communications providers are also expected to implement appropriate signalling gateway and interconnectivity frameworks and associated overload control mechanisms.

4.62 The proposed guidance sets out a number of measures that we expect communications providers to 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;[67]

[65] ESO. *Electricity System Restoration Standard.* https://www.nationalgrideso.com/industry-information/balancing-services/electricity-system-restoration-standard [accessed 5 December 2023].
[66] The user plane in networking is the part of the network that is responsible for carrying user traffic, such as web pages, videos, and voice calls. It is also known as the data plane or forwarding plane.
[67] This could be done by ensuring that control plane functions are situated across different locations, each with multiple active connections.

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.

4.63 Communications providers are also expected to take measures at the control plane to:

a) avoid signalling overload at Customer Premise Equipment (CPE), and other user equipment (4.3.2);
b) ensure that network functions with 'real-time charging' interfaces take resilience and reliability into account in their designs and testing (4.3.3); and
c) 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).

Why we consider these measures in the control plane are appropriate and proportionate.

4.64 We explain above that 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.

4.65 We consider that the measures we set out in our proposed guidance for the control 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.

4.66 In designing our proposed 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[68] and NICC[69].

4.67 The proposed guidance includes resilience measures that represent best practice in that they are featured in several GSMA guidelines documents that are used by communications providers across the world. The proposed guidance also includes references to those best practice approaches which should be considered by communications providers to help ensure that resilience is optimised at the control plane aspects of their network, and which contain further examples of the mechanisms and frameworks which communications providers could implement in order to ensure they are meeting their security duties.

---

[68] 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].

[69] 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].

4.68 For example, the GSMA documents referred to in the proposed guidance provide guidance and requirements on how to design, operate, and secure mobile network to network interfaces (NNI) and user to network interfaces (UNI)[70] for interoperability, optimal performance, reliability, and security.[71]

4.69 The proposed guidance also refers to guidance 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.[72] The objective of this task group, and the practices it prescribes, are to inform communications 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.[73]

4.70 The proposed 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.

4.71 We have recorded a number of control plane incidents. One incident led to a communications provider's customers being unable to register onto the network and led to 3.5 million customer-hours being lost.[74]

4.72 We recorded further control plane incidents at a separate communications 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).

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

4.74 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.

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

---

[70] '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.

[71] 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*.

[72] 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.

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

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

4.76 A separate communications 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.

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

4.78 We should also note that any recommended measures included in the proposed 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 communications provider to assess what aspects of the proposed 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 communications 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.

4.79 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.

4.80 We also consider that the proposed measures will not produce adverse effects which are disproportionate to the aim pursued. In addition to the proactive engagement mentioned in 4.52, as part of Ofcom's Incident Reporting function, following network and service outages, Ofcom has undertaken significant engagement with communications 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 communications providers that operate with relatively smaller user bases e.g., alternative network providers.

4.81 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 communications providers. However, the post-incident engagements, where incidents resulted in significant network and service outages, have highlighted examples where we consider communications 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 proposed guidance, we seek to clarify our expectations on appropriate and proportionate measures that communications providers should take in relation to their network design and operational models. In most cases, following incident reviews with Ofcom, communications providers have implemented appropriate changes to their networks or services to prevent, or minimise, the likelihood of future occurrences.

4.82 Our view is that communications providers who follow this 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…'*.[75]

[75] NICC, 2023. *ND 1657 SIP- Overload Control*. p7

4.83 Therefore, we regard the proposed 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.

Question 2: Do you consider the measures in the proposed guidance relating to the resilience at the Control Plane to be appropriate and proportionate?

Management plane resilience

4.84 *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.

4.85 The management plane can be implemented using a dedicated management network, which is separate from the main data network relied on by end user. This is described as 'out-of-band' (OOB) management.[76] This helps to protect the management plane from being affected by traffic on the main data network but also avoids the management plane impacting on the data network.

4.86 The proposed guidance (section 4.4.1) emphasises the benefits of having an OOB management function available for key network equipment. It enables communications providers to carry out critical tasks even when the main network goes down. For example, having a dedicated network allows a communications provider to restore services on multiple and geographically dispersed sites if they fail, meaning that time consuming and labour intensive 'van 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.

4.87 The PSTN has sometimes been used as a method for out of band access, using analogue lines or ISDN lines, based on the logic that it was built before modern transmission and IP networks, and therefore should be physically separate to them.

4.88 With PSTN switch off, communications providers will need to give consideration to alternative methods, or risk losing OOB management functionality. Multiple options are available depending on the communications provider's needs. For example, there are options based on PON[77] and 4G/5G connectivity which could provide this function for some operators. Although we do not prescribe in detail what method of OOB management should be used because the best option for a given communications provider is likely to vary.

Why we consider these measures in the management plane are appropriate and proportionate.

4.89 We explain above that 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.

[76] The management plane may be provided 'in-band' over the same production network as the user and signalling plane with appropriate separation, or 'out-of-band' (OOB) separate from the primary network carrying the user and signalling plane.
[77] Passive Optical Network

4.90 We consider that the measures we set out in our proposed 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.

4.91 In designing our proposed 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 have written about network and IT systems management including: ISO[78], ITIL[79], ETSI[80], ITU[81], ENISA[82], EC-RRG[83], NRIC[84], TMN[85], COBIT[86], etc.

4.92 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 Communications 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.'*[87]

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

4.94 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 out of band 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.

4.95 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, they 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

---

[78] 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.
[79] The Information Technology Infrastructure Library (ITIL) (discussed further at 4.129)
[80] The European Telecommunications Standards Institute is a standards development organisation that develops standards for information and communication technologies.
[81] The International Telecommunication Union is an international organisation within the United Nations where Member States and business coordinate global telecom networks and services.
[82] European Union Agency for Cybersecurity (ENISA) is the European Union's centre of expertise in cybersecurity.
[83] 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.
[84] The Network Reliability and Interoperability Council is an advisory committee to the Federal Communications Commission (FCC) on telecoms network reliability and interoperability.
[85] The Telecommunication Management Network is a protocol model defined by the International Telecommunication Union (ITU-T) for managing open systems in a communications network.
[86] 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.
[87] EC-RRG, 2021. *EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure.* p30. Section 8.2.1

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'.[88]

4.96 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 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.'[89]

4.97 The FCC report goes on to say, '*T-Mobile implemented this best practice as a corrective action to prevent a recurrence of this event*'.[90] We note that the best practice they refer to has been in place since at least 2011.[91]

4.98 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.[92] 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.'[93]

4.99 These experiences, and particularly the impact that these have had on end users, further strengthens our view that the requirements included within the proposed guidance are appropriate, and necessary to avoid unacceptably high levels of risk of significantly high loss of connectivity to end users. If communications providers implement the measures included in the proposed 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

---

[88] Meta, 2021. *More details about the October 4 outage*. https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/ [accessed 22 November 2023].
[89] Federal Communications Commission, 2020. *June 15, 2020 T-Mobile Network Outage Report*. p17 para 45.
[90] Ibid
[91] 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.
[92] 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*
[93] Federal Communications Commission, 2019. *A Report of the Public Safety and Homeland Security Bureau Federal Communications Commission August 19, 2019.* p15 para 40

outlined above, would be greatly reduced, or such incidents would have a less severe impact.

4.100 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.

4.101 In preparing the measures outlined in the management plane guidance, Ofcom has been mindful to avoid specifying what communications providers should do in detail. For example, we have not sought to prescribe the implementation of a particular type of OOB management system. Instead, we recognise that communications providers should introduce OOB management solutions that are tailored to the nature and scale of their own network. For example, relatively small communications 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 communications providers, with multiple sites, it is likely that such a manual approach would be impractical. We would therefore expect these larger communications providers to adopt a more scalable OOB system to better meet their management needs. We consider that this approach allows communications providers to only implement those of our described measures which are necessary to fulfil their security duties under s105A-D in a given instance.

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

4.103 Ofcom has also undertaken significant engagement with communications providers to understand what measures they currently take at the management plane. Our conclusion from these engagements is that most of these communications providers do run some form of OOB management system already, mostly based on the PSTN. As the PSTN is set to be de-commissioned over the next few years, we would expect communications providers to be increasingly focussed on adopting alternative solutions.

4.104 Our view is that most communications 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 proposed guidance measures at the management plane as proportionate.

Question 3: Do you consider the measures in the proposed guidance relating to the resilience of the Management Plane to be appropriate and proportionate?

Resilience for a communications provider's own services

4.105 The scope of the proposed guidance extends beyond just the underlying infrastructure of communications providers' networks. It also applies to the services that many communications 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 communications provider managed services.[94]

4.106 The proposed guidance explains that communications providers will 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 are singled out in the proposed guidance as being 'a specialised service'.

4.107 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 contended. This can lead to a slowdown in network traffic at certain pinch points in the network.

4.108 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.

4.109 Voice service prioritisation can also help with the regulations requiring communications providers to provide end users with access to emergency services, introduced to ensure the availability of fixed voice services when contacting emergency services.[95]

4.110 The proposed guidance also sets an expectation that communications providers design, host, and operate primary 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 provided but can also have the additional benefit of reducing cyber threats. The guidance also requires that communications providers make provision for fast and scalable failure detection and failover mechanisms to minimise any negative impact to communications provider managed services that may result from resilience failures.

Why we consider the resilience measures for communications providers' managed services are appropriate and proportionate

4.111 We explain above that 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.

4.112 We consider that the measures we set out in our proposed guidance for the communications providers' managed services are appropriate to achieve this aim as, if these

[94] This term should not be confused with the process of contracting out some, or all, of a company's workload to a separate third party.

[95] Ofcom. *General Conditions of Entitlement*. https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/telecoms-competition-regulation/general-conditions-of-entitlement#:~:text=A3%3A%20Availability%20of%20services%20and,uninterrupted%20access%20to%20emergency%20organisations [accessed 22 November 2023]. General Condition A3 is a regulatory obligation on communications providers take all necessary measures to ensure uninterrupted access to emergency organisations for their customers. This condition aims to ensure the fullest possible availability of public communications services at all times, including in the event of a disaster or catastrophic network failure, and uninterrupted access to emergency organisations.

measures are not taken by communications providers, there is an unacceptably high risk of significant loss of connectivity for end users.

4.113 In designing the proposed guidance relating to the provision of communications 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 communications providers to take in order to meet their resilience related security duties.

4.114 The proposed guidance refers to 3GPP and GSMA standards that prescribe for the separation of voice and internet traffic on *mobile* networks and devices.[96] The proposed 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.[97]

4.115 Given the risks associated with network congestion at various parts of a communications 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 primary voice services are prioritised to ensure end users have reliable access to voice calls during emergency situations.

4.116 The measures included in the proposed guidelines 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 proposed 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.[98]

4.117 The proposed guidance measures offer communications providers with enough flexibility to allow them to take action proportionate to their situation and goes 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 communications 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 proposed guidance therefore recognises that

---

[96] 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]

[97] 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*.

[98] 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.

communications providers must make choices that align with their service design requirements and obligations.

4.118 We also consider that the proposed measures will not produce adverse effects which are disproportionate to the aim pursued. The measures outlined are regarded as standard practice among most major communications 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 communications providers not being able to provide a service at all, or with significant impairments to voice call quality.

Question 4: Do you consider the measures in the proposed guidance relating to communications providers' own managed services to be appropriate and proportionate?

Processes, tools and training

4.119 The proposed guidance also sets 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 (section 5). These expectations are summarised below.

Network and service design

4.120 When communications providers are introducing new services, or making changes to existing ones, the proposed guidance (section 5.1.1) sets 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, and have plans to resume services quickly. The proposed guidance sets out measures for communications providers to have management processes in place to monitor and configure service levels, capacity, availability, continuity, and supplier management. The proposed guidance also describes some of the tools that communications providers can use to support these management activities.

Network and service transition

4.121 The proposed guidance reminds communications providers that the deployment of both new services, and updates to existing ones, require careful consideration, planning and testing. The proposed guidance (section 5.2) sets out a number of management practices that should be considered as part of network and service transition. These include having:

a) a robust change management plan[99]
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.

4.122 The proposed guidance advises caution when communications 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.

[99] The change management plan should be able to answer a number of key questions about transition risks, timings and the testing regime.

Service operation

4.123 Service operation relates to managing a service through its day-to-day production life. The proposed guidance (section 5.3) sets out a number of management requirements that communications 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.

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

Skills competency training

4.125 The proposed guidance (section 5.4) reminds communications providers that staff competency is key to supporting resilient systems and processes. The proposed guidance explains 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.

Why we consider the guidance measures in the processes, tools and training section are appropriate and proportionate

4.126 We explain above that 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.

4.127 We consider that the measures we set out in our proposed guidance in relation to processes, tools and training are appropriate to achieve our 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.

4.128 In designing our proposed 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.

4.129 Of particular relevance to these aspects is the Information Technology Infrastructure Library (ITIL).[100] 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 proposed guidance, that match those in the ITIL framework, is an appropriate means to ensure that

[100] 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].

communications providers can implement delivery across their organisations in a resilient way.

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

4.131 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.

4.132 Additionally, over the course of the reporting period 2022/23, 20 incidents were reported to Ofcom, each with impacts exceeding 1 million user hours of lost service. Of these incidents, the top three have a root cause within 'change control' and 'change management'. This includes an incident 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'.

4.133 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.

4.134 There are also examples from outside of the UK where communications providers have experienced significant issues that may have been avoided if the practices outlined in the proposed 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.

4.135 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 was caused while a core network router was being replaced as part of its regular maintenance.[101] 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.

4.136 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

[101] Kiddi Corporation, 2022. *The July Communication Failure and Our Response.* https://www.kddi.com/english/important-news/20220729_01/ [accessed 22 November 2023].

recovery procedures when congestion occurs and Development of tools to recover congestion at VoLTE Nodes'.

4.137 Whilst our proposed 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 communications 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.

4.138 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.[102] The causes of the outage are subject to an ongoing investigation by the Canadian regulator. However, 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.'*[103]

4.139 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'.[104]

4.140 The FCC's review of the 2020 T-Mobile incident in the US, referenced above at 4.46, again provided lessons for communications 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 work months prior to the date of the outage but could have been identified in a test environment:

'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.'[105]

4.141 Our proposed guidance includes specific measures relating to 'Testing and Validation Management'. Our view is that such testing in controlled environments, ahead of any

---

[102] 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].

[103] 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].

[104] 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].

[105] Federal Communications Commission, 2020. *June 15, 2020 T-Mobile Network Outage Report.* p16 para 45.

planned network changes, may reduce the likelihood of events such as those referenced above from occurring.

4.142 These experiences, and particularly the impact that these have had on end users, further strengthens our view that the requirements included within the proposed guidance are appropriate.

4.143 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.

4.144 As mentioned above, Ofcom has been mindful to avoid prescribing standardised measures that apply uniformly across all use cases and communications providers. The proposed guidance around change management, training, asset identification and management and life cycle management can all be tailored to communications providers of all types and sizes. Further, the proposed guidance has been drafted in a way to ensure communications 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 communications 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 communications providers with a helpful steer as to how they can build resilient networks, though still allowing for a high degree of flexibility in decision making.

4.145 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 our guidance provides should allow communications providers to improve their process, tools, or training in a way that efficiently improves resilience. Therefore, we regard these aspects of the proposed guidance to be proportionate.

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

4.147 As mentioned above, Ofcom has undertaken significant engagement with communications 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. These discussions inevitably involved enquiries about the processes, skills and training in place at these communications providers, which are needed to support the various network aspects mentioned above.

4.148 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 communications providers. However, the post-incident engagements, where incidents resulted in significant network and service outages, have highlighted examples where we consider communications 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 proposed guidance, we seek to clarify our expectations on appropriate and proportionate measures that communications providers should take in relation to processes, skills and training. In most cases, following incident reviews with Ofcom, communications providers have implemented appropriate changes to prevent, or minimise, the likelihood of future occurrences.

Question 5: Do you consider the measures in the proposed guidance relating to communications providers' arrangements for preparing for adequate process, skills and training to be appropriate and proportionate?

5. Call for Input: ensuring power resilience in mobile radio access networks

Summary

5.1 We use this section to set out a call for input on ensuring power resilience at the mobile RAN. At this stage, we have not included measures relating to the provision of additional power backup up at the mobile RAN in the proposed guidance.

5.2 As outlined in Section 2, reliable communications services are essential to our everyday lives and to the economy. A key ongoing risk to the mobile networks is the availability of mains electrical power. Interruptions to mobile services could mean consumers cannot make emergency calls, contact friends or family, or go online. Currently, the amount of existing electrical power backup within the mobile access networks varies. Below we set out the wider context, and consider how the issue of sufficient power backup could be addressed through regulation.

5.3 We lay out a framework for assessing which measures would be appropriate and proportionate for MNOs to take to comply with their resilience related security duties under s105A-D of the Communications Act 2003 in order to manage the risk of power outages which have a detrimental impact on consumers by preventing access to communications services.

5.4 Our work to date suggests the high costs involved in providing a minimum of one hour of backup power resilience at every cell site could mean it is not possible to conclude whether this would be a proportionate measure at this time. The one-hour figure is based on initial evidence from Ofgem on the average duration of power outages.[106]

5.5 Given this, we are inviting stakeholders' input, including on what services consumers should be able to expect during a power outage, and what a more cost-effective solution could look like to address potential consumer harm. We want to start a discussion about what power backup MNOs can and should provide for their networks and services, with a view to implementing this in our guidance in the future, and/or working with industry and Government to identify and pursue other ways to address this issue.

Context

5.6 The UK's energy network is generally resilient, but communications providers can, and do, experience energy outages. As noted in Section 2, the UK's growing use of, and reliance on, communications services means that the consequences of energy outages which in turn compromise the availability, performance or functionality of networks and services are increasingly acute.

[106] See Annex A2

5.7 Ofcom's own incident reporting shows that between 2020 and 2022, 693 out of 2735 (25.3%) of the reported incidents for fixed and mobile networks were caused by power-related issues. Further that and 245 days' worth of incidents out of a total of 1393 days (17.6%) were power related.[107,108]

5.8 The amount of existing electrical power backup within mobile access networks varies. Some MNOs have a small number of cell sites with several hours or days' worth of power backup, often at remote sites or 'hub' cell sites, which other 'child' cell sites rely on.[109] Some, but not all MNOs also have power backup in some form at all of their sites (of a minimum of 10-15 minutes). As noted below, data from Ofgem shows that the vast majority of power outages that affect consumers are relatively short. Where power outages are limited to a specific area, consumers may receive coverage from another nearby cell site with overlapping coverage.

5.9 In recent years, the UK has experienced a number of extreme weather events. This has highlighted the challenge of the power resilience for communications networks and the need for cross sector collaboration to prepare for these events and improve response times to manage their negative effects. For example, over the winter 2021/22, a series of severe storms with high winds hit the UK, resulting in power outages. The impact on communication services was particularly severe in those areas where the loss of power meant that mobile cell sites failed. These outages also affected customers' fixed line services. Some were left without any means to communicate, including making calls to the emergency services.

5.10 Preparing for, and responding to, severe storms requires a multi-pronged approach by fixed and mobile communications providers. This includes implementing a wide range of processes, such as incident management and business continuity plans, as well as cross-sector work with energy distribution network operators (DNOs) on power restoration processes. The power recovery process following the winter 2021/22 storms highlighted the need for better co-ordination and information sharing between the communication and energy sectors. To some extent, steps taken since, have helped to reduce the overall impact and recovery times resulting from storms. We want to see further progress being made by communications providers in their collaboration with the power industry. The simultaneous loss of access to all fixed and mobile forms of communication in a region as a result of severe weather remains on the Government's National Risk Register[110].

5.11 Storms are not the only cause of power outages, and the current migration of landline users from PSTN to VoIP technology means that some will become more reliant on mobile networks in the event of a power outage that reduces availability of fixed networks.[111] We are likely to see a further shift of consumers from traditional landlines to VoIP-based telephone services that use a broadband connection. Ofcom's existing guidance under

---

[107] Ofcom, Connections Nations Data 2020-2022, communications network or service incidents.
[108] This information is based on incidents above a minimum threshold that are reported to Ofcom in line with section 5 of Ofcom's General Statement of policy (Ofcom. *General statement of policy under section 105Y of the Communications Act 2003*. p20-33. Section 5)
[109] Hub or 'parent' sites transmit data from smaller 'singleton' or 'child' sites to core sites.
[110] HMG, 2023. *National Risk Register*. p93
[111] Unlike some traditional corded analogue phones, a digital phone will only work in a power cut if it has a battery back-up: Ofcom, 2023. *Moving Landline Phones to Digital Technologies.* https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/future-of-landline-calls [accessed 22 November 2023]

General Condition A3.2(b) states that providers must have at least one solution available that enables access to emergency organisations for a minimum of one hour in the event of a power outage at the customer's premises.[112] In response, communications providers are deploying a number of solutions including in-home battery backup units.[113] Some communications providers are providing 'hybrid handsets' that rely on a mobile signal to make calls, including those to emergency services, in the event of an outage. This means that an increasing number of consumers relying on VoIP technology, will likely turn to their mobile network in the event of a power outage, including to make an emergency call.[114] More broadly, 35 million 999/112 calls were made in 2021, of which 74% were from a mobile and 26% from a landline.[115]

5.12 It could be argued that the only appropriate approach to securing a resilient power supply, particularly for mobile networks, would be to increase the resilience of the power distribution network. There are arrangements for providing increased resilience and redundant power feeds for certain CNI assets.[116] Whilst MNO RANs could increasingly be viewed as CNI assets, at present it is not clear they would qualify under the existing framework, and legislative change may be required.[117] The current approach to power resilience for CNI assets, which is based on separate electricity distribution network infrastructure, does not lend itself to the scope and scale of mobile access networks which are distributed throughout every area of the UK.

5.13 Technology at the mobile RAN is also rapidly evolving in a way that can affect and reduce power consumption as well the increase the efficiency of power backup solutions over coming years. Newer technologies are more power efficient – one terabyte delivered using 5G technology consumes only 7% as much power as one terabyte delivered using 3G technology.[118] MNOs could focus power backup on newer technologies such as 4G and 5G. MNOs could also look to develop their network data analytics and dynamic optimisation to tune their networks to reduce power consumption (as well as the associated costs and carbon impact), enabling batteries to last longer. For example, it may be possible to effectively turn off higher frequency bands to maintain coverage using lower frequency bands for longer, at the expense of throughput capacity.[119]

---

[112] This must be provided free of charge to customers who are dependent upon their landline, for example they do not own a mobile phone or have no mobile signal at home, to call emergency services during a power cut. General Condition A3.2 requires all regulated providers to take necessary measures to ensure communications in catastrophic network breakdown or force majeure, and that there is uninterrupted access to emergency services as part of publicly available telephony services: Ofcom, 2018. *Protecting access to emergency organisations when there is a power cut at the customer's premises*.

[113] Many battery backup units designed to meet the nominal one-hour requirement can last for longer if usage is restricted and industry are now developing and deploying solutions which can last several hours.

[114] Some newer handsets can fallback to other means of communication in emergencies such as satellite

[115] 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].

[116] BEIS, 2019. *Electricity Supply Emergency Code*

[117] From Ofcom's understanding, MNOs have not requested redundancy through the Protected Site Process of the Energy Supply Code.

[118] Vodafone, *We're switching off our 3G network.* https://www.vodafone.co.uk/help-and-information/3g-switch-off [accessed 22 November 2023].

[119] Within the Telecom Infra Project there are a variety of technical options being investigated, developed, and tested to optimise mobile 5G Radio Access Networks. Some of these optimisations include innovations in

International examples of widespread power backup range from MNOs' own initiatives to regulatory intervention and public funding.

5.14 To better understand the challenge of power resilience at the mobile RAN, we have looked at international comparisons, and will continue this research and engagement.

5.15 Overseas regulators, such as NKOM in Norway, and Traficom in Finland, have introduced specific power backup up regulations. The requirements in Norway can vary on the location of the cell site but look to ensure the continuity of mobile services in the event of a power outage. NKOM require 2 hours in densely populated areas and 4 hours in less populated areas. [120] The duration of power backup required can vary between different countries. Traficom, requires 4 or more hours in densely populated areas, and 6 hours or more in less populated areas.[121] Some other regulators have not, to date, provided specific regulatory requirements, but have proposed other measures to ensure power resilience at the mobile RAN, such as the German regulator Bundesnetzagentur.[122]

5.16 Some overseas MNOs have been seeking to ensure power resilience at the mobile RAN absent of regulation, such as A1 in Austria.[123] Indeed, some have gone further and taken the opportunity to capture, store, and sell energy back to the grid. Following Traficom's decision to implement specific backup regulations for all RAN sites, MNO Elisa Polystar are extending their Distributed Energy Storage solution with funding from the Finnish government.[124] This allows Elisa to purchase and store energy during periods of low demand, and lower per unit cost, and sell stored energy during periods of high demand to the Finnish national grid at the market rate.[125] This indicates the potential additional financial benefits that MNOs may be able to achieve.

---

energy efficiency and spectrum management. These developments could potentially extend the time that a given amount of battery backup could last, if the RAN was reoptimized. The Telecom Infra Project (TIP) is a global community of companies and organisations working together to accelerate the development and deployment of open, disaggregated, and standards-based telecoms infrastructure solutions: Telecom Infra Project, 2023. https://telecominfraproject.com/ [accessed 22 November 2023]

[120] Nasjonal Kommunikasjonsmyndighet, 2020. *Tilbyders sikkerhets- og beredskapsplikter.* https://nkom.no/sikkerhet-og-beredskap/tilbyders-sikkerhets-og-beredskapsplikter#minstekrav_til_reservestrmkapasitet_i_mobilnett [accessed 22 November 2023]. Original text in Norwegian.

[121] Traficom, 2020. *Regulation on resilience of communications networks and services and of synchronisation of communications networks: Explanatory Notes*. p34-35

[122] Bundesnetzagentur, 2020. *Strategiepapier: Resilienz der Telekommunikationsnetze.* p12. Original text in German. Proposed measures include providing backup power to enough base stations to provide full coverage and the restriction of mast capabilities to low band (700 to 900 Hz) only. The mast use restriction would allow for an extended length of coverage so long as there is even a limited amount of power that can be supplied.

[123] A1 Telekom Austria is a fixed and mobile network operator in Austria. Der Standard, 2022. *Blackout: Nach 30 Minuten geht dem Mobilfunk der Saft aus*. https://www.derstandard.at/story/2000139672819/blackout-nach-30-minuten-geht-dem-mobilfunk-der-saft-aus [accessed 22 November 2023]. Original text in Austrian German.

[124] Traficom, 2020. *Regulation on resilience of communications networks and services and of synchronisation of communications networks: Explanatory Notes*. p34-5

[125] Elisa, 2023. *Elisa to accelerate Distributed Energy Storage solution*. https://elisa.com/corporate/news-room/press-releases/elisa-to-accelerate-distributed-energy-storage-solution-%E2%80%93-europe%E2%80%99s-largest-distributed-virtual-power-plant-in-the-making/64851337650499/ [accessed 22 November 2023]

5.17 The Australian Government launched a targeted, publicly funded intervention to enhance power backup-up provision. This includes measures taken at 467 base stations through the first round of its 'Mobile Network Hardening Program'. These typically rural and remote sites have been fitted with 12 hours power backup up capability. Further rounds of funding to extend capacity and improve resilience across more sites are currently underway. [126]

We are seeking input on how power resilience of mobile networks could be improved in the UK

5.18 The UK Government's April 2023 Wireless Infrastructure Strategy noted that the Secretary of State for the Department of Science, Innovation and Technology (DSIT) has asked Ofcom to review how communications providers are meeting the needs of their customers in regard to the power resilience of mobile networks in the event of an outage.[127]

5.19 We acknowledge the measures already being taken by Government, Ofgem, and the energy industry, to further improve the resilience of energy networks.[128] However, we consider additional steps are required to address the resilience of sectors, such as communications, which are dependent on energy supply to provide essential services. We want to work collaboratively with others, mentioned above, to mitigate the impact of power outages on communications services.

5.20 As noted in Section 4, in the fixed access network, and in both fixed and mobile 'core' network domains, existing approaches to ensuring power backup appear to be broadly consistent.

5.21 For RAN sites, the availability of power backup up is less consistent across MNOs, and we expect there to be complex reasons driving this. We would like to start a public discussion about what power backup measures MNOs can, and should, take on the RAN. This is with a view to including RAN power backup measures in our resilience guidance in the future, and/or working with industry and Government to identify and pursue other options.

5.22 As set out in Section 2, Ofcom's aim is to secure the provision of networks and services which are robust, available, and working well. Communications providers have a duty to take appropriate and proportionate measures in order to maintain the availability, performance or functionality of their networks and services under s.105A and C of the Communications Act 2003. Ofcom has a general duty, under s.105M of the 2003 Act, to seek to ensure that communications providers comply with their security duties. In the context of these duties, we have prepared a framework for assessing which measures are appropriate and proportionate for a provider to take in order to comply with their duties under s.105A and C, with respect to mobile RAN cell sites. We refer to those providers that have security duties in respect of such sites (be it as an operator, infrastructure provider or otherwise) as Mobile

[126] Australian Government, Department of Infrastructure, Transport, Regional Development, Communications and the Arts. *Mobile Network Hardening Program*. https://www.infrastructure.gov.au/media-communications-arts/phone/mobile-network-hardening-program#:~:text=Round%201%20of%20the%20Mobile,resilience%20of%20regional%20telecommunications%20infrastructure [accessed 22 November 2023].
[127] DSIT, 2023. *UK Wireless Infrastructure Strategy*. p.26
[128] Ofgem, 2022. *Ofgem confirms local electricity networks price control for 2023 to 2028* [accessed 22 November 2023].

Network Operators ("MNOs")[129]. Our framework contains a series of questions covering the types of outages communications providers can be expected to prepare for, the impact on consumers, the backup technologies available, operators' existing approaches, and the feasibility and costs of upgrades.

5.23 To help inform this work, we have gathered some initial evidence on the average duration of power outages (see annex A2), existing practices, and the costs of upgrades, as detailed below. Using the framework below, and drawing upon the evidence to hand, our illustrative example suggests that to install a minimum one hour of battery power backup on RAN sites, where power backup is likely to be feasible, could cost in the region of £0.9 - £1.8bn. This high cost means that it is difficult to conclude that it is proportionate to the aim in this case, to include such a measure in our proposed guidance at this stage. We are therefore inviting stakeholders' input on what actions generally can, and should, be taken in order to improve power resilience of the mobile RAN, in order to best achieve our aim. We recognise that some of these may lay outside the scope of current regulation, and a combination of solutions may be required over coming years. To start this discussion, we are inviting input on what services consumers should be able to expect during a power outage that affect MNOs, and what a more cost-efficient solution could look like, such as identifying a set of sites that could provide ongoing coverage, or the maintenance of a reduced service level (including emergency services access via voice, SMS, or video relay).

5.24 We welcome continued input from the Energy Networks Association and Ofgem to aid understanding of historical and likely future UK power outages. We also welcome MNOs' input so far on the costs associated with increasing power backup to RAN sites and services and encourage further feedback through this CFI on their approach to making their networks resilient. We will also engage further with international regulatory counterparts to build on our understanding of best practice.

A framework for assessing appropriate and proportionate measures for power backup for mobile networks

5.25 As set out in Section 3, under s.105A CA03, providers of PECN and PECS have 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.

5.26 In this section, we set out a framework for considering the various factors which are relevant to assessing what measures are appropriate and proportionate for MNOs to implement in relation to the power backup of their RAN. This framework considers the key factors that drive consumer harm from outages and the costs and feasibility associated with mitigating that harm.

5.27 We then set out an illustrative example and questions for stakeholders to consider.

[129] We note that there are a number of providers of neutral host solutions, who operate RAN cell sites which interconnect into the four large MNO networks for the provision of PECS. Where these providers are providing PECN, they are required to comply with the security duties set out in s105A-D and implement appropriate power resilience.

Our framework

5.28 Our framework considers the following factors:

a) What types and duration of power outages can MNOs be expected to prepare for?

b) What is the impact of consumers not being able to access communications services as a result of power outages to RAN cell sites?

c) What role do individual RAN cell sites play in the wider network or service availability?

d) What are operators' existing approaches?

e) What power backup technologies and technical options could be deployed at RAN cell sites?

f) What is the feasibility of improving and upgrading sites?

g) What are the potential costs of improving current levels of power resilience?

5.29 We have set this out in more detail to better examine the different elements of the problem and the evidence available, as well as to identify where further information is required to move this complex issue forward. We expand upon this below and invite comments.

Framework factors	Considerations for each factor
a) what types and duration of power outages can MNOs be expected to prepare for?	There are multiple scenarios in which mains electrical power may not be available to MNOs: i. Short term power outages that can last for a few minutes to up to a few hours. ii. Power surges and lulls: fluctuations in the power supply of the main public power grid can impact electronic equipment connected to it, including in the RAN. Having power backup smooths out these fluctuations and ensures equipment is more protected.[130] iii. Events such as severe weather can affect power supply across a region for many hours to days in extreme cases, as outlined in the National Risk Register.[131] iv. National Grid resilience planning provides for more extreme situations such as multi day power outages across the UK or rota disconnections.[132] Communications providers should seek advice from the Government and from the National Grid Electricity System Operator (ESO) regarding such power disruptions.[133]

[130] 61 power surges were reported to us in the last year, which resulted in approximately 4.3m customer hours lost.

[131] HMG, 2023. *National Risk Register*. p97

[132] Rota disconnections seek to reduce the impact of a national energy shortage by implementing staggered power outages across specified regions. If required, the National Electricity Grid Electricity System Operator (ESO) will legally order DNOs to shut down power in a process set out in the Government's Electricity Supply Emergency Code: National Grid, 2023. *Rota Load Disconnections*. https://www.nationalgrid.co.uk/rota-load-disconnections#:~:text=How%20would%20rota%20disconnections%20work,for%20most%20of%20the%20day [accessed 22 November 2023]

[133] For example, see 'Failure of the National Electricity Transmission System (NETS'). HMG, 2023. *National Risk Register*. p95

Framework factors	Considerations for each factor
b) what is the impact of consumers not being able to access communications services as a result of power outages to RAN cell sites?	Consumers could lose a range of communications services during a power outage. As outlined in Section 2, consumers increasingly rely on communication services for many aspects of their lives. In the event of a power outage that impacts both fixed and mobile communications services, consumers and most businesses could be unable to contact the emergency services, family and friends, or go online to communicate, work, or access information. The geographical extent and duration of an outage would affect the extent to which consumers could access communications services. i. Depending on how wide an outage is over a given area, and the infrastructure affected, a consumer may be able to use a power resilient digital landline as an alternative to mobile, providing the consumer does not use a cordless landline device.[134] If an outage is limited to a particular mobile cell site or small area, consumers may receive mobile coverage from a nearby overlapping cell site. ii. Whilst some activities such as contacting emergency organisations can be time critical, other activities can be delayed until power and communications are restored (e.g., some business activities and streaming entertainment services). [135,136.] iii. Where a power outage affects homes, having resilient communication networks also allows consumers to report power outages to energy companies. [137.] iv. The Government's Emergency Alert System also relies on 4G mobile cell sites to broadcast alerts to compatible mobile devices.[138]

[134] Although as PSTN services are replaced by Voice over Internet Protocol (VoIP) based call services delivered over broadband, this capability will be lost unless on premises power resilience is available. For landline-dependant consumers, following Ofcom guidance, some communications providers have provided battery backup units to ensure premises power resilience. Additionally, those consumers on copper-based broadband services may not be affected by power outages: Ofcom, 2018. *Protecting access to emergency organisations when there is a power cut at the customer's premises*

[135] Defined as the police, fire, ambulance, and coastguard services.

[136] In 2021 Ofcom mandated that communications providers should provide Emergency Video Relay Calls, which requires data services to be used: Ofcom, 2022. *Emergency Video Relay*. https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/telecoms-industry-guidance/how-will-emergency-video-relay-work [accessed 22 November 2023].

[137] Utilities also need to communicate during emergency situations so that supply is restored as soon as possible. To meet its operational communication needs, the utilities sector uses a mix of public and private, wired and wireless networks. However, the sector expects to see growth in its communication requirements, with the biggest changes in the electricity sector which is transforming to support net zero. A number of technology and network solutions could play a role in meeting this increasing demand; one option being advocated by the energy industry is a new private communication network (using 4G/LTE or 5G) which would require access to suitable spectrum in part or all of the UK. If a private network was deemed necessary for utilities, the potential candidate spectrum bands to enable this are discussed in June 2023 Ofcom call for input. Ofcom, 2023. *Call for Input: Potential spectrum bands to support utilities sector transformation.*

Framework factors	Considerations for each factor
c) What role do individual RAN cell sites play in the wider network or service availability?	The extent of backup required at any location should be determined considering a combination of: i. how many customers are served by the network domain in question; ii. its location; and iii. the extent to which that part of the network could be a single point of failure, or whether an alternative connection is available; and iv. the extent of that connection (i.e. whether the customer will still receive a full service or emergency calls, SMS, or video relay only). RAN sites are by nature dispersed. The number of customers served by a cell site is not static. A single site can reach hundreds or thousands of consumers, and all RAN sites require power to function. The wider the area affected by a power outage, the higher the likelihood a consumer cannot receive a service from an overlapping cell site or a fixed connection.
d) What are operators' existing approaches?	A consideration of what an appropriate and proportionate level of power resilience should be for RAN, is an operator's existing starting point - the level of power resilience it currently provides; what strategic choices have been made in the past regarding power backup, and more broadly, what industry baseline exists.
e) What power backup technologies and technical options could be deployed at RAN cell sites?	The choice of any backup power technology for a particular site will depend on the location and power consumption of the network component and particular technologies it needs to serve. In some cases, it is possible for the power consumption of a particular technology to be reduced, meaning a battery would last for longer (see context).

https://www.ofcom.org.uk/consultations-and-statements/category-1/potential-spectrum-bands-to-support-utilities [accessed 4 December 2023].

[138] Local resilience forums (LRFs) and response groups, also rely on public mobile phone networks. HMG. *How Emergency Alerts Work*. https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/telecoms-industry-guidance/how-will-emergency-video-relay-work [accessed 22 November 2023].

Framework factors	Considerations for each factor
f) What is the feasibility of improving and upgrading RAN sites?	The extent of power resilience will be shaped and potentially constrained by what it is practical and feasible to include at any one site. Factors which affect feasibility include: i. Location and size of a site and space for [additional] power backup; for example core sites with room for generators, or in access networks, whether street furniture has room to house battery strings in existing cabinets or new cabinets are required; ii. For sites located at the top of buildings, the weight of any new equipment; iii. Permission, ease of access and planning rules; whether a communications provider owns a site or new permissions from landlords are required to add additional equipment, and whether that equipment is subject to limitations under planning rules, for example in street cabinets.
g) What are the potential costs of improving current levels of power resilience?	The total costs of maintaining existing equipment and of installing any additional power resilience will involve costs including: i. Planning and sending an engineer to install new batteries and integrate them into the network domain to ensure smooth switch from mains to backup power when required. ii. The specific power backup equipment (including the battery strings as well as the racks and cabinets needed to store the battery strings). iii. Maintenance, monitoring, and loading fees.

CFI question 1: Does this framework accurately capture the factors relevant to assessing what is an appropriate and proportionate measure for MNOs to take with regards to power resilience for RAN cell sites?

Illustrative example applying the framework to RAN

5.30 As an illustrative example, we provide below some inputs and suggested answers to the key policy questions (a) and (b) within the framework. We then draw these together with the technical questions (c) to (g) into an initial assessment. If (a) and (b) were to be answered differently, this would shape any conclusions about cost effective solutions (either in a proportionality assessment by Ofcom, or outside of existing regulation). So, we invite stakeholders' input on each of these questions.

a. What types and duration of power outages and issues can MNOs be expected to prepare for?

5.31 At a minimum, it is expected that mobile RAN sites should be able to operationally withstand short term power-related incidents.

5.32 Whilst preparing for, and responding to, severe storms requires cross sector collaboration, including to ensure rapid power restoration, installing battery power backup for short term incidents would also provide some incremental benefit for an initial period during outages related to extreme weather events.

5.33 However, to provide benefit for longer durations during such outages, the installation of greater levels of power backup at one easily accessible site within a particular area (such as a train station), may be appropriate to provide a designated service capability for the region.

5.34 Using customers or metered supply connection points as a proxy for RANs, Ofgem data (see Table 1) suggests that the majority of customers impacted by outages of over 3 minutes, are impacted for outages of 3 mins to 1 hour.

CFI question 2: Do you agree that at a minimum MNO's networks should be able to operationally withstand short term power-related incidents of an hour at RAN sites?

b. What is the impact of consumers not being able to access communications services as a result of power outages to RAN cell sites?

5.35 Power outages at cell sites can cause harm to those consumers whose communications services rely on that site and fail as a result of the power cut. The harm experienced can range from less serious harm (e.g., an inability to access recreational content), to much more serious harm (e.g. the inability to communicate during an emergency or to carry out essential work, or access health or financial services) in any given case. While we recognise that there may 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.

5.36 In the context of their security duties, we consider that MNOs should be generally robust and seek to maintain a normal level of service, both in the provision of voice calls and the provision of internet services, during a power outage. This would minimise the harm caused to consumers, and the wider economy, through the loss of communications services during a power outage.[139]

CFI question 3: What mobile services should consumers be able to expect during a power outage, what consumer harms should power backup up focus on mitigating and does this vary depending on the type or duration of the outage? [140]

[139] We note that there is a separate requirement relating to the availability of PECN/PECS under General Condition A3 which aims to ensure the fullest possible availability of public electronic communications services at all times, including in the event of a disaster or catastrophic network failure. This also requires uninterrupted access to emergency organisations.

[140] Our analysis here is focussed on the needs of the mass market but it is worth noting that there are wider "resilience" impacts from commercial MNO service failures. Power companies and other "Level 2 Responders" under the Civil Contingencies Act do rely on such services to mobilise and coordinate their activities and service outages will have an impact on their ability to deal with major events, as Storm Arwen demonstrated. HMG and NIC have identified that the implications of this do need to be assessed and Ofcom is supporting this work in a number of ways.

c. What role do individual RAN cell sites play in the wider network or service availability?

5.37 RAN sites ensure consumers' access to the network; all sites require power to function and some sites ('hubs') are needed to transmit traffic from dependent child sites back to the core.

5.38 A consumer's service during a power outage will be dependent on the extent of overlapping coverage from adjacent cell sites and the geographical breadth of a power outage. Any site could be affected by a power outage.

d. What are operators' existing practices?

5.39 The amount of existing electrical 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).

e. What power backup technologies and technical options could be deployed at RAN cell sites?

5.40 Where power backup is deployed, it is generally through batteries, except in very isolated areas. Power consumption depends on a number of factors including the function of the site (e.g. at hub sites, transmission data connecting smaller singleton or 'child' sites back to the network core represents a lower portion of data than local data carrying traffic directly from and to consumers), the technology being used, and the number of customers attached at any one time.[141]

5.41 Newer RAN technologies are increasingly more efficient in power consumption.[142] MNOs may be able to make technical choices over time to reduce power consumption to optimise their RAN usage (see context section).

> **CFI question 4**: What technical choices are available to MNOs to reduce power consumption, and should be considered as part of assessment of appropriate and proportionate measures?

f. What is the feasibility of improving and upgrading RAN sites?

5.42 It is feasible to back up many, but not all sites, given restrictions on weight and planning restrictions. For example, planning restrictions around street furniture mean communications providers may be restricted as to the size and thus duration of batteries that can be installed on any given site. Considerations include permission, ease of access and

[141] Hub or 'parent' sites transmit data from smaller 'singleton' sites to core sites.
[142] ARCEP, 2022. *Energy assessment of 4G vs. 5G deployment.*

planning rules; whether a communications provider owns a site or new permissions from landlords are required to add additional equipment, and whether that equipment is subject to limitations under planning rules, for example in street cabinets.

CFI question 5: How many sites would it be feasible to upgrade and maintain and why?

g. What are the potential costs of improving current levels of power resilience?

5.43 Across the four large UK MNOs, we estimate that to backup all RAN sites that can feasibly have 1hr power backup would incrementally cost between £0.9 -£1.8bn.[143] We have gathered and assessed cost estimates from all four MNOs, noting that some operators caveated their estimates as preliminary and potentially understated.

5.44 In most cases, operators provided estimates for power backup lasting more than one hour. Noting that the majority of energy customers impacted by outages of over 3 minutes, are for outages of 3 mins to one hour, we have adjusted their estimates to determine the potential incremental cost of one hour power backup.

5.45 We estimate that it could cost £20-25k per site to have one hour power backup per site, which includes both capital costs and multiple years of additional operating costs modelled over the economic life of the cell sites.

5.46 We then estimate that it would be technically feasible to provide 1 hour backup to between 44k and 70k sites.

5.47 The 44k lower bound also excludes sites that we consider to be unlikely to accommodate 1 hour battery backup as well as sites that already have at least 1 hour backup. If only 44k sites were backed up, some sites would be excluded, so quality of service would likely be reduced (at least for data services).[144]

5.48 Combining these two ranges we estimate 1 hour power backup at all feasible RAN sites to cost between £0.9- £1.8bn.

Initial assessment – illustrative example

5.49 Looking at the above analysis, our starting point is that in order to meet their security duties, MNOs should take at least some measures to mitigate against the risks of power outages and support continued communications services during short term power outages and surges which might reasonably be expected to occur. This will help to reduce the detrimental impact on consumers of such outages.

5.50 In order to achieve this, we consider that MNOs should implement some form of power backup at their mobile RAN sites (where feasible). The next step would be to determine what level of power backup up it is appropriate and proportionate for communications providers to provide.

[143] This is in cash terms and using current prices.

[144] However, we expect the 52k sites would represent the vast majority of sites that can feasibly have at least one hour power backup and ensure nearly full coverage of the UK.

5.51 The indicative data we have gathered suggests that a minimum of 1 hour power backup at a given RAN site would address the majority of customer hours lost in energy outages (where energy customers are a proxy for access networks). See Annex A2. This would reduce disruption and harm to consumers from the loss of communications services.

5.52 Given the risk that any mobile RAN sites might be affected by a power outage, arguably the minimum necessary to achieve sufficient power backup to support continued communications services during short term power outages and surges would be to implement this level of backup at all mobile sites, where feasible. However, we recognise that the costs of doing so are likely to be substantial, over £1 billion across the industry for 1 hour backup. These significant indicative costs mean we cannot necessarily conclude that to recommend such a measure in our proposed guidance would be proportionate at this time.

CFI question 6: Do you consider that providing a minimum of 1 hr backup to all RAN cell sites would to be proportionate to meet the security duties under s.105A to D of the Communications Act 2003?

5.53 Investing in greater power backup at mobile RAN sites would benefit from economies of scale, i.e., the cost per hour reduces as the number of hours increases. At the same time, we would not expect the overall benefits per hour to necessarily reduce so 4 hours backup would roughly provide quadruple the benefits of 1 hour.[145] This suggests that 4 hours backup is more likely to be proportionate than 1 hour backup, at least on a per site basis.

5.54 Given this, we welcome stakeholders' input on what other cost-effective solutions may be found to meet consumers' needs during a power outage. We have listed some initial options below but welcome stakeholders' wider suggestions. We recognise that some of these may lay outside the ambit of current regulation, and a combination of solutions may be required over coming years:

5.55 A subset of cell sites could be identified for enhanced power backup – such as those sites that are at a higher risk of a power outage (these may also be at risk of longer outages).

5.56 A subset of cell sites could be identified as those sites that are necessary to maintain some basic level of service on each MNO's network (e.g., voice, SMS, video relay access to 999, and a basic data service). MNOs would be best placed to suggest how such cells be identified.

5.57 A co-ordinated optimisation of power resilient UK emergency call and SMS coverage could be introduced, which would require battery backup across different MNO RANs.

5.58 One MNO could be designated a network of last resort to provide emergency call service to consumers.

CFI question 7: What cost effective solutions do you consider could meet consumers' needs during a power outage?

CFI question 8:

[145] We note that there could be cases where the value per hour reduces with each additional hour (e.g., where there is a decreasing propensity to require service continuity), whilst there could be other cases where the value per hour increases.

a) Is it more cost efficient to increase power backup up to any space, weight, or planning limitations, i.e., increasing power backup as much as is feasible provides the lowest £ per hour?

b) do the benefits of any power backup solution have diminishing returns, i.e., the benefit per hour decreases as you increase the amount of power backup?

CFI question 9: Does the mobile market fail to capture the value or importance of power backup, and if so, why?

CFI question 10: Should improvements in power backup be focused on solutions at sites which are identified as higher risk of outages?

CFI question 11: Why would any requirement lower than a minimum of 1 hour be sufficient in future? What duration do you consider would be sufficient and why?

CFI question 12: Over what time period could industry make upgrades to provide a minimum of 1 hour at every cell site or other cost-effective solutions to address potential consumer harm?

A1. Impact Assessment

A1.1 Section 7 of the Communications Act 2003 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.

A1.2 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 'Better policy-making': Ofcom's approach to impact assessment'sets out our general approach to how we assess and present the impact of our proposed decisions. [146]

A1.3 The relevant duties in relation to the proposal on which we are consulting are set out in Section 3 (the legal framework). The analysis presented in this document constitutes an impact assessment as defined in section 7 of the Communications Act 2003. Our analysis of the likely impact of our proposals is contained throughout Section 4 and Section 5. This includes the impact of the implementation of the measures included in the proposed guidance (insofar as they are not already implemented by providers) at the physical network infrastructure domains (4.37 – 4.54, and 4.55 - 4.58), the control plane (4.64– 4.83), the management plane (4.89 – 4.104), communications providers' own services (4.111 – 4.118), and processes, tools, and training (4.126 - 4.148).

A1.4 We also consider that communications providers will benefit from the proposed guidance as they will have further clarity on how we expect them to meet their resilience related security duties.

A1.5 We expect these proposals to result in an overall positive impact for consumers, citizens and business by ensuring more reliable communications and internet services that meet the need for increased societal demand for them. We have assessed this proposal against the alternative, the retention of the 2022 Guidance which would remain in place, but provides significantly less detail. The proposed Guidance sets out those changes which we consider would most effectively and proportionately satisfy our objectives (Sections 4.2 - 4.9) compared to that counterfactual.

A1.6 We are seeking to open a broader discussion with industry and the government on RAN power backup. We have not provided specific recommendations on the extent to which power backup should be implemented at the RAN level, nor included this within our updated guidance. Consequently, it has not been necessary a comprehensive impact assessment of the proposals in this respect.

Impact on Communications Providers

A1.7 Our proposed update to the guidance aims to provide additional clarity for communications providers regarding their duties under s105A-D and ensure that the guidance both reflects the changing nature of resilience risks and is future proofed (Sections 4.4 – 4.4).

[146] Ofcom: 'Ofcom's approach to impact assessment', (2023).

A1.8 Whilst we recognise that there may be some additional costs associated with communications 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. Measures contained in the guidance are flexible enough to apply to all types of communications providers offering communications networks and services in the UK, while also allowing for continued technology evolution, and communications providers may choose to comply with their resilience-related security duties by adopting different technical solutions or approaches to those specified.

A1.9 We also expect that this flexibility and the technology and network agnostic positioning of our proposed measures (Sections 4.16 – 4.17) will limit the impact on competition of the proposed guidance. In addition, we consider the use of customer hours lost helps to ensure that smaller providers are not disproportionality impacted by our proposed guidance measures.

Impact on citizens, consumers, and businesses

A1.10 Our proposed guidance aims to improve the resilience of communications providers in a way that the benefits to citizens and consumers. Any additional costs that might be passed on to them is likely to be outweighed by the benefits to citizens and consumers that comes from a reduction in service outages and costumer hours lost, and improved service quality.

Equality Impact Assessment

A1.11 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. [147]

A1.12 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.

[147] Ofcom, 'Revised Northern Ireland Equality Scheme for Ofcom' ,(2019).

A1.13 We do not consider that our proposals 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 proposed guidance relates to the measures to be taken by all providers of PECN/PECSs, 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 more rurally, when for example, we have proposed that when considering network architecture, design, and operational models, we expect communications 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 communications providers.

A2. Ofgem data

A2.1 We have gathered some initial evidence on the average duration of power outages which we have detailed below. We welcome further input on relevant information through this document.

Duration of power outages (of outages above 3 minutes)

A2.2 Table 1 below describes data provided by Ofgem that lists the proportion of customers impacted by power outages in each of the duration bands listed, in Great Britain (GB). This national picture is likely to vary for different geographical locations.

A2.3 'Customers' in this context is defined as 'a metered supply connection point', which would typically include the supply to a RAN cell site. This data, provided by Ofgem, is based on supply interruptions on distribution networks as recorded in the National Fault & Interruption Reporting Scheme (NaFIRS) database.

A2.4 A reported interruption is when supply has been off, or not adequate, for a total of 3 minutes or longer. Outages of less than 3 minutes are not included in the provided data. Ofgem have informed us that the frequency of transient interruptions of less than 3 minutes outweighs the other bandings. Therefore, this table does not represent the total number of power outages experienced, and should not be interpreted as doing so. However, it does provide important context to the frequency of power outages, where the ability to access communications services may be impacted by its duration.

A2.5 This data suggests that around two thirds of outages experienced by customers, that last over 3 minutes, are resolved within an hour.

Table 1 GB Domestic power outage duration percentages. Source: Ofgem.

Year	2018/19	2019/20	2020/21	2021/22	2022/23
Below 3 mins	No data				
3 minutes - 1 hour	65%	66%	67%	61%	65%
1 - 2 hours	19%	18%	18%	17%	19%
2 -3 hours	6%	6%	6%	6%	6%
3 - 6 hours	6%	6%	6%	7%	6%
6 - 12 hours	3%	3%	3%	4%	3%
12 - 18 hours	0%	0%	0%	1%	0%
18 hours +	0%	0%	0%	3%	0%

A3. Responding to this consultation

How to respond

A3.1 Ofcom would like to receive views and comments on the issues raised in this document, by 5pm on 1 March 2024.

A3.2 You can download a response form from https://www.ofcom.org.uk/consultations-and-statements/category-1/resilience-guidance-mobile-ran-power-back-up. You can return this by email or post to the address provided in the response form.

A3.3 If your response is a large file, or has supporting charts, tables or other data, please email it to resilience.team@ofcom.org.uk , as an attachment in Microsoft Word format, together with the cover sheet.

A3.4 Responses may alternatively be posted to the address below, marked with the title of the consultation:
CP Resilience Team (Network and Communications Group)
Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA

A3.5 We welcome responses in formats other than print, for example an audio recording or a British Sign Language video. To respond in BSL:

- send us a recording of you signing your response. This should be no longer than 5 minutes. Suitable file formats are DVDs, wmv or QuickTime files; or
- upload a video of you signing your response directly to YouTube (or another hosting site) and send us the link.

A3.6 We will publish a transcript of any audio or video responses we receive (unless your response is confidential)

A3.7 We do not need a paper copy of your response as well as an electronic version. We will acknowledge receipt of a response submitted to us by email.

A3.8 You do not have to answer all the questions in the consultation if you do not have a view; a short response on just one point is fine. We also welcome joint responses.

A3.9 It would be helpful if your response could include direct answers to the questions asked in the consultation document. The questions are listed at Annex 6. It would also help if you could explain why you hold your views, and what you think the effect of Ofcom's proposals would be.

A3.10 If you want to discuss the issues and questions raised in this consultation, please contact resilience.team@ofcom.org.uk

Confidentiality

A3.11 Consultations are more effective if we publish the responses before the consultation period closes. This can help people and organisations with limited resources or familiarity with the issues to respond in a more informed way. So, in the interests of transparency and good regulatory practice, and because we believe it is important that everyone who is interested in an issue can see other respondents' views, we usually publish responses on the Ofcom website at regular intervals during and after the consultation period.

A3.12 If you think your response should be kept confidential, please specify which part(s) this applies to and explain why. Please send any confidential sections as a separate annex. If you want your name, address, other contact details or job title to remain confidential, please provide them only in the cover sheet, so that we don't have to edit your response.

A3.13 If someone asks us to keep part or all of a response confidential, we will treat this request seriously and try to respect it. But sometimes we will need to publish all responses, including those that are marked as confidential, in order to meet legal obligations.

A3.14 To fulfil our pre-disclosure duty, we may share a copy of your response with the relevant government department before we publish it on our website.

A3.15 Please also note that copyright and all other intellectual property in responses will be assumed to be licensed to Ofcom to use. Ofcom's intellectual property rights are explained further in our Terms of Use.

Next steps

A3.16 Following this consultation period, Ofcom plans to publish a statement in summer 2024.

A3.17 If you wish, you can register to receive mail updates alerting you to new Ofcom publications.

Ofcom's consultation processes

A3.18 Ofcom aims to make responding to a consultation as easy as possible. For more information, please see our consultation principles in Annex 4.

A3.19 If you have any comments or suggestions on how we manage our consultations, please email us at consult@ofcom.org.uk . We particularly welcome ideas on how Ofcom could more effectively seek the views of groups or individuals, such as small businesses and residential consumers, who are less likely to give their opinions through a formal consultation.

A3.20 If you would like to discuss these issues, or Ofcom's consultation processes more generally, please contact the corporation secretary:

A3.21 Corporation Secretary
Ofcom
Riverside House
2a Southwark Bridge Road
London SE1 9HA
Email: corporationsecretary@ofcom.org.uk

A4. Ofcom's consultation principles

Ofcom has seven principles that it follows for every public written consultation:

Before the consultation

A4.1 Wherever possible, we will hold informal talks with people and organisations before announcing a big consultation, to find out whether we are thinking along the right lines. If we do not have enough time to do this, we will hold an open meeting to explain our proposals, shortly after announcing the consultation.

During the consultation

A4.2 We will be clear about whom we are consulting, why, on what questions and for how long.

A4.3 We will make the consultation document as short and simple as possible, with an overview of no more than two pages. We will try to make it as easy as possible for people to give us a written response.

A4.4 We will consult for up to ten weeks, depending on the potential impact of our proposals.

A4.5 A person within Ofcom will be in charge of making sure we follow our own guidelines and aim to reach the largest possible number of people and organisations who may be interested in the outcome of our decisions. Ofcom's Consultation Champion is the main person to contact if you have views on the way we run our consultations.

A4.6 If we are not able to follow any of these seven principles, we will explain why.

After the consultation

A4.7 We think it is important that everyone who is interested in an issue can see other people's views, so we usually publish the responses on our website at regular intervals during and after the consultation period. After the consultation we will make our decisions and publish a statement explaining what we are going to do, and why, showing how respondents' views helped to shape these decisions.

A5. Consultation coversheet

Basic details

Consultation title:

To (Ofcom contact):

Name of respondent:

Representing (self or organisation/s):

Address (if not received by email):

Confidentiality

Please tick below what part of your response you consider is confidential, giving your reasons why

- Nothing ☐
- Name/contact details/job title ☐
- Whole response ☐
- Organisation ☐
- Part of the response ☐

If you selected 'Part of the response', please specify which parts:

If you want part of your response, your name or your organisation not to be published, can Ofcom still publish a reference to the contents of your response (including, for any confidential parts, a general summary that does not disclose the specific information or enable you to be identified)?

Yes ☐ No ☐

Declaration

I confirm that the correspondence supplied with this cover sheet is a formal consultation response that Ofcom can publish. However, in supplying this response, I understand that Ofcom may need to publish all responses, including those which are marked as confidential, in order to meet legal obligations. If I have sent my response by email, Ofcom can disregard any standard e-mail text about not disclosing email contents and attachments.

Ofcom aims to publish responses at regular intervals during and after the consultation period. If your response is non-confidential (in whole or in part), and you would prefer us to publish your response only once the consultation has ended, please tick here.

Name Signed (if hard copy)

A6. Consultation questions

Proposed guidance consultation questions

Question 1: Do you consider the measures in the proposed guidance relating to the resilience of the physical infrastructure domains to be appropriate and proportionate?

Question 2: Do you consider the measures in the proposed guidance relating to the resilience at the Control Plane to be appropriate and proportionate?

Question 3: Do you consider the measures in the proposed guidance relating to the resilience of the Management Plane to be appropriate and proportionate?

Question 4: Do you consider the measures in the proposed guidance relating to communications providers' own managed services to be appropriate and proportionate?

Question 5: Do you consider the measures in the proposed guidance relating to communications providers' arrangements for preparing for adequate process, skills and training to be appropriate and proportionate?

Call for Input questions

CFI question 1: Does this framework accurately capture the factors relevant to assessing what is an appropriate and proportionate measure for MNOs to take with regards to power resilience for RAN cell sites?

CFI question 2: Do you agree that at a minimum MNO's networks should be able to operationally withstand short term power-related incidents?

CFI question 3: What mobile services should consumers be able to expect during a power outage, what consumer harms should power backup up focus on mitigating and does this vary depending on the type or duration of the outage?[148]

CFI question 4: What technical choices are available to MNOs to reduce power consumption, and should be considered as part of assessment of appropriate and proportionate measures?

CFI question 5: How many sites would it be feasible to upgrade and maintain and why?

[148] Our analysis here is focussed on the needs of the mass market but it is worth noting that there are wider "resilience" impacts from commercial MNO service failures. Power companies and other "Level 2 Responders" under the Civil Contingencies Act do rely on such services to mobilise and coordinate their activities and service outages will have an impact on their ability to deal with major events, as Storm Arwen demonstrated. HMG and NIC have identified that the implications of this do need to be assessed and Ofcom is supporting this work in a number of ways.

CFI question 6: Do you consider that providing a minimum of 1 hr backup to all RAN cell sites would to be proportionate to meet the security duties under s.105A to D of the Communications Act 2003?

CFI question 7: What cost effective solutions do you consider could meet consumers' needs during a power outage?

CFI question 8:

a) Is it more cost efficient to increase power backup up to any space, weight, or planning limitations, i.e., increasing power backup as much as is feasible provides the lowest £ per hour?

b) do the benefits of any power backup solution have diminishing returns, i.e., the benefit per hour decreases as you increase the amount of power backup?

CFI question 9: Does the mobile market fail to capture the value or importance of power backup, and if so, why?

CFI question 10: Should improvements in power backup be focused on solutions at sites which are identified as higher risk of outages?

CFI question 11: Why would any requirement lower than a minimum of 1 hour be sufficient in future? What duration do you consider would be sufficient and why?

CFI question 12: Over what time period could industry make upgrades to provide a minimum of 1 hour at every cell site or other cost-effective solutions to address potential consumer harm?

A7. Proposed Guidance

A7.1 The proposed guidance can be found on this link.