

Voxyonder welcomes the opportunity to provide feedback to Ofcom's Resilience Guidance Consultation.

NOTE: This response to the consultation is based on our interpretation and understanding of the current supplier, technological, regulatory and policy landscape as is and may be subject to change.

In this consultation when referring to CP, PECN or PECS unless the context makes clear otherwise, we are referring to a fixed voice CP, PECN, PECS (i.e not mobile or broadband) targeted primarily at B2B rather than B2C, but in certain contexts can also include B2C. Furthermore, when referring to the Act unless the context requires otherwise we are referring to the Communications Act 2003¹ and when referring to Regulation unless the context requires otherwise we are referring to the Electronic Communication (Security Measures) Regulation 2022². Where we relate to Code of Practice, this is in relation to the Telecommunications Security Code of Practice³.

This consultation is segmented into 3 parts:

- Overview
- Our Concern around Internet Interconnection Proposals
- Answers to other Ofcom's Questions

Overview

Overall, we are mostly in agreement with the majority of aims, suggestions and desired outcomes of the guidance. We appreciate it is difficult to issue guidance in a way which covers such a wide spectrum of Communications Provider types (Mobile, Broadband, Fixed Voice) and credit Ofcom on the whole for what we consider as reasonable expectations of any CP (regardless of type). However, we feel based on the consultation and it's accompanying guidance there are some gaps within the understanding of how smaller fixed voice CPs operate their services and an overall misunderstanding of the scale and importance of the public internet among smaller fixed voice CPs (or potentially any fixed voice CP who is not vertically integrated and does not provide the physical transport link to the customer). It is worth factoring in that smaller CPs (most likely fixed voice CPs) by volume make up the majority of all CPs in the market. This is somewhat reinforced by DCMS survey data⁴ and Ofcom numbering data⁵. Furthermore, as highlighted by DCMS in regards to the Regulation impact assessment, it is difficult to estimate how many CPs there actually are⁶.

¹ <https://www.legislation.gov.uk/ukpga/2003/21/contents>

² <https://www.legislation.gov.uk/uksi/2022/933/contents/made>

³ https://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf

⁴ <https://www.gov.uk/government/publications/telecommunications-providers-survey-october-2021-to-february-2022/telecommunications-providers-survey-october-2021-to-february-2022-research-notes>

⁵ <https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/numbering/numbering-data>

⁶ https://www.legislation.gov.uk/ukia/2022/74/pdfs/ukia_20220074_en.pdf - 6.19

In our view, we believe there to be at least 1,000 PECNs and several thousand more PECSs as defined by the Act, along with public data available through Ofcom's numbering data⁵, Ofcom ADR data⁷ and DCMS⁴ which we believe the majority of these are fixed voice CPs. It is also worth remembering Ofcom encourages CPs to suballocate numbering to other CPs⁸ so there is likely to be many more multiples of PECNs who do not have allocated ranges themselves than PECNs who do.

Therefore, it is important for any guidance not to materially directly or indirectly (i.e. that which will be enforced contractually via larger CPs) negatively affect smaller fixed Voice CPs to the point they cannot continue to operate due to undue operational pressures or their operations are no longer economically viable. In doing so in itself could cause sectorial integrity issues far beyond what this guidance is attempting to avoid.

Our Concern around Internet Interconnection Proposals

In summary we have significant concerns regarding the guidance⁹ issued in 4.2.4 which states *"voice/VoIP/IMS interconnection between networks should be separate from the Internet"* and the statement issued in the consultation¹⁰ at 4.110 that CPs *"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."* We do see potential solutions that we would consider as a reasonable middle ground which are discussed later.

Our concerns (which we will expand on) are:

- Does not seem to acknowledge how, in our view, a large portion of fixed voice CPs operate;
- Goes beyond the Regulation and Code of Practice;
- Could cause a reduction in Innovation, landline traffic and a consolidated market;
- Will put larger CPs as the gatekeepers of these requirements meaning smaller CPs could be cut off and impacted to make operational changes based on their topology setup;
- The Pro's of public internet interconnection are not considered;
- We feel there is a knowledge gap regarding how smaller CPs operate;
- There are inconsistencies between interpretations of standards;
- Lack of consideration of solutions around internet interconnection and solutions;

⁷ <https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/problems/adr-schemes>

⁸ https://www.ofcom.org.uk/__data/assets/pdf_file/0022/247504/annex2-good-practice-guide.pdf

⁹ https://www.ofcom.org.uk/__data/assets/pdf_file/0024/272931/Network-and-Service-Resilience-Guidance-for-CPs.pdf

¹⁰ https://www.ofcom.org.uk/__data/assets/pdf_file/0023/272930/Consultation-Resilience-guidance-and-mobile-RAN-power-back-up.pdf

That being said, taking into consideration the concerns raised in the consultation, our view point and concerns raised by some in the wider voice sector historically (which we also share), the issue around internet interconnection does need reviewing in a way that manages risks, but also does not stifle market participants, innovation or cost to entry. It's not uncommon for a small new entrant CP to enter the market utilising virtual machines and dedicated servers rather than operating via colocation estate.

We believe recent policy interventions by Ofcom (on how UK CLI is used and its limited use cases outside of the UK¹¹) and DCMS (Regulation 4(5) on encryption¹²) will in part resolve some of these concerns. Furthermore, we agree that where large volumes of voice are carried over an interconnect, then this must be via a non-internet based method. However, for lower volumes we believe (given the other policy interventions which will enhance the confidentiality of the interconnection voice traffic) the risk to be low and an internet interconnection can actually enhance resilience. Therefore, we feel public internet interconnections should be permitted where the overall voice volume on the interconnect link is expected to be < 5,000,000 minutes per month or 500 concurrent calls (which ever is higher) and this limit is per interconnection link between switches. In our view, intra UK internet interconnectivity is consistently low latency, very low jitter and many CPs operate at least in part their own public IP network and thus have control over how internet traffic routes in/out of their network and many given their setups peer over internet exchanges allowing for a high quality connection over a public peering option. Some CP strategies use multiple data centres and ISP suppliers to increase resilience while typically larger or more embedded CPs invest in colocation estate, but for smaller CPs who may only have a very small customer base, this may not be economically viable.

Likewise, smaller and larger CPs who operate internet accessible voice services can incorporate a wide range of strategies that reduce and mitigate security compromise.

Many businesses (especially since Covid) utilise voice services via the public internet and arguably, in our view, if it were not for these services would have severely limited the UKs response to how businesses (including the public sector) handled the pandemic. It's generally seen as one of the benefits of the migration to all-IP voice. Otherwise, if we're looking for closed loop systems which by nature is more secure by design and has increased resilience guarantees against power outages and uninterruptible voice, then the PSTN which is currently being shut down in our view was the solution for that. We in part agree with your views in 4.5.1 of the guidance and especially footnote 38 around internet based VoIP not able to meet some of the high standards expected in a 'Primary-Line' and there are policies in place to mitigate potential issues that have only just been reminded and recommunicated to CPs by Ofcom with their obligations¹³.

We question on your exact meaning by a primary-line and primary voice service as you have not (unless we've missed it) defined what a primary-line and primary voice service are. Our current interpretation of what we think you mean by a primary voice line/service

¹¹ <https://www.ofcom.org.uk/consultations-and-statements/category-2/improving-cli-data-accuracy>

¹² <https://www.legislation.gov.uk/uksi/2022/933/regulation/4/made>

¹³ https://www.ofcom.org.uk/_data/assets/pdf_file/0030/264846/open-letter-999-programme.pdf

is any voice line where emergency services can be called, which essentially then applies to most voice services.

Over the past 10-15 years, there have been thousands of fixed voice PECS come to market. Some are mainstream and some fulfil a niche requirement. In our view, a large portion of these smaller fixed voice PECS outside the physical cable landline connection relied in some way on the public internet, be it the internet being the method of accessing the PECS or the CPs PECN being hosted among virtual machines or dedicated servers utilising public internet interconnection between them and other CPs.

Finally, we note that your approach appears to be evidence led (which we not considering as bad, we feel this is a major positive). However, given the reporting threshold for security incidents are high for smaller CPs¹⁴, it is unlikely smaller CPs would meet the thresholds to report and thus would have limited view of them. In addition, only a small number of CPs responded overall to the consultation on the Electronic Communication (Security Measures) Regulation 2022¹⁵. Of those who responded, only a very limited number of those represent smaller Fixed Voice CPs. This reinforces our view that smaller CPs somewhat go under the radar when policy is considered and smaller businesses generally (not just CPs) seldomly get involved in government or regulatory consultations, yet actually make up by volume an important part of the fixed voice market. Typically, in many previous consultations gone by this has never been an issue when any proposed policy typically effects CPs equally regardless of size. But impact assessments should be conducted in more detail where the burdens may disproportionately impact smaller suppliers more and we believe this will actually happen should the guidance come into effect as you've defined it.

Goes further than the Regulation code of practice

We believe the guidance for interconnection goes further than the Code of Practice. From our understanding by 2028¹⁶ voice traffic going over the interconnection should be encrypted (i.e. encrypting the Signal to reduce security compromises, whereby voice traffic over the interconnect would be the meaning under Section 32 of the Act)^{17 18}. This guidance requires interconnection to not be over the internet, yet makes no reference (as far as we can see) to encryption. This seems to be a step backwards, whereas during the draft consultation of Regulation 4(4) it referred 'or otherwise'¹⁹ in an attempt to reduce

¹⁴ https://www.ofcom.org.uk/_data/assets/pdf_file/0021/51474/ofcom-guidance.pdf - Table 1

¹⁵ <https://www.gov.uk/government/consultations/proposal-for-new-telecoms-security-regulations-and-code-of-practice/outcome/proposals-for-new-telecoms-security-regulations-and-code-of-practice-government-response-to-public-consultation#annex-b-list-of-respondents> – Annex A

¹⁶ https://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf - Signalling Plane 4 – 31st March 2028.

¹⁷ <https://www.legislation.gov.uk/uksi/2022/933/regulation/4/made> - Regulation 4(5)

¹⁸ <https://www.legislation.gov.uk/uksi/2022/933/regulation/2/made> - Signal - S 32(10) - CA2003

¹⁹ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/951726/Draft_Electronic_Communications__Security_Measures__Regulations.pdf - Regulation 4(4) - "A network provider must use within the public electronic communications network signals which, by encryption or otherwise, reduce the risks of security compromises."

security compromise (e.g. our understanding was to utilise encryption to protect the Signal or another method that would reduce security compromise (e.g. a physical connection)). Then, in the main consultation this was later removed, implying that in the context of interconnects should be encrypted regardless of medium or transport layer. Relating to this, from our understanding CPs have until 2028 to enable the Code of Practice around this¹⁶. We would like clarification on when Ofcom would expect CPs to migrate their internet interconnect to outside of the internet. The 2028 deadline relies on CPs having to update their interconnection protocol with no change in transport layers (overall this is a lot of work given the volume of interconnects that are likely to exist).

We note that although the document is guidance, the guidance makes it clear CPs should have a very good excuse for any deviation on their part and when it comes to looking at enforcement action will be used as a starting point (Proposed Guidance 1.1).

For many voice CPs, a major change to the interconnection transport layer will have a substantial impact affecting a large portion of Fixed Voice CPs (especially those with infrastructure based on Virtual Machine and Dedicated Services outside of any CP managed colocation setup).

Furthermore, this interconnection related policy undermines the spirit of the Regulation whereby small CPs (i.e. micro-entities) and in some respects Tier 3's enjoy a significantly reduced burden, but this interconnection policy proposal introduces logistical problems whereby these micro-entities and tier 3's interconnect with tier 2's and 1's.

Reduction in Innovation, Landline Traffic and a consolidated Market

In our view, we believe the UK has one of the most, if not the most, competitive and innovative CP eco systems of any country.

We note in several areas you imply that you want to continue the promotion of innovation in the sector, yet a significant amount of this innovation has occurred because CPs have had an affordable, easy way to come to market without needing to invest in significant amounts of infrastructure or complex interconnectivity agreements. In our view, the majority of the innovation over the past few years in the fixed line voice sector has been due to smaller CPs. We only need to look at the rapid over-night UK transition to a work from home environment and how these CPs (especially smaller CPs) had come to market with solutions within days to meet this requirement.

We believe the suggested changes could increase the speed of reduction in landline voice traffic in the UK based on CPs being unable to meet the interconnection requirements and internet based access services being frowned upon. If many CPs were to leave the market either voluntarily or other interconnecting networks contractual enforcing proposed interconnection guidelines, it could shut off other networks ultimately resulting in sectorial wide integrity issues (also breaking the concept of porting among the public) and furthermore is unclear how CPs other obligations (e.g. those around SMP and porting) will be met. We ask whether Ofcom and DSIT would be ready

for a wide range of CPs leaving the market (voluntarily or non-voluntarily) in a short space of time.

The changes around interconnection we feel could potentially put Ofcom in breach of its own obligation under Section 3 of the Act²⁰ as we cannot see how this policy decision could be implemented without causing a material impact in PECS (and those PECN's whose PECS operate on) from leaving the market. Equally given the reduction in market participant size and thus competition, it would not promote the interest of the overall public.

Given the points raised in 4.5-4.9 of the consultation, our belief is that you're implying this guidance document for enforcement action purposes should be treated as sacrosanct unless there is a serious reason why a CP is not to be compliant with it.

Furthermore, we are concerned that the consultation and guidance creates an impression of discrediting and/or devaluing what are perceived to be internet based fixed voice services whereby, in our view a large portion, if not the majority of end users in non-vertically integrated setups utilise fixed line voice services over an internet connection (especially those focusing in the B2B part of the market. E.g. SIP Trunking).

Larger CPs will be the gatekeepers for raising Standards

We note that in 4.13 and 4.52 of the consultation you claim to have consulted with a wide range of CPs, although we ask how many of these were Tier 3 or Micro-Entity fixed line voice CPs and of that proportion, how many are access networks as defined by Ofcom?²¹

Furthermore in 4.17 you highlight what may be appropriate and proportionate for a larger CP, may not be that for a smaller CP. Although, given the criticality of interconnection between smaller and larger CPs (especially the several hundred CPs that have SMP obligations upon them) and larger CPs having higher security requirements than smaller CPs (through the Regulation and Code of Practice), it is unrealistic and impractical to expect a larger CP (in our view) to deviate from your guidelines to accommodate a smaller CP, therefore putting a smaller CPs and larger CPs in a very difficult position. Therefore, compromises are required.

Pro's and Con's of Internet Interconnection

Our belief falls contrary to your comment in 4.36 and we see the benefits of interconnection over the internet for resilience purposes is overall better as there will be multiple paths the voice data packet can take in the event of a supplier transit failure. However, there are mechanisms which will protect the contents of the Signal coming into effect by 2028. Furthermore, given the commercial models of interconnection, internet

²⁰ <https://www.legislation.gov.uk/ukpga/2003/21/section/3>

²¹ https://www.ofcom.org.uk/__data/assets/pdf_file/0029/216794/statement-2021-26-wholesale-voice-markets-review.pdf - Footnote 109

connectivity allows for easier and more cost-effective connectivity by increasing the resilience for access to the terminating number range and overall geo diversity resilience among smaller simpler setup CPs. It also increases competition (reducing costs) within the wholesale sector which then feeds through to the customer (retail).

Furthermore, security concerns have been raised by sector stakeholders prior about the potential of billions of minutes traversing the public internet unencrypted potentially leaving the UK to come back^{22 23 24}. We totally agree this is unacceptable, but unfortunately the horse has long bolted (10+ years ago). However, recent policy interventions by DCMS/DSIT and Ofcom should, in our view, provide a reasonable middle ground (i.e. voice should be encrypted through Regulation 4(5) and given the recent changes around the use of CLI²⁵, then there are limited situations when UK voice traffic may involve networks outside the UK). We appreciate this is the typical cybersecurity argument of security versus usability. What could be viewed a minor change in Ofcom's eyes could cause major supplier difficulty in a very short space of time whereby it's thought there could be well over 1,000 PECNs (and several thousand more voice PECS on those PECNs) based on public DCMS and Ofcom data. It would also affect the Wholesale Voice Market.

If Ofcom proceeds with these policy changes without a realistic timetable (at a minimum at least on par with the 2028 deadline of encryption to allow a reasonable adjustment time and potential solutions to come to market that allow those without a physical colocation setup to migrate). We would firmly propose urgent further research to be undertaken by the department to better understand the important role smaller fixed voice CPs play in providing some of the most innovative voice solutions (such as those consumed by the public and private sector).

Furthermore, regarding your point in 4.36 of the consultation, we fail to see how CPs are expected to Interconnect with International CPs if not over public internet where it's impractical, unreasonable and for the most part not even possible to interconnect with an international CP without a public internet connection (especially for smaller CPs).

Our view point on Interconnect Security Standards

In point 4.110 of the consultation, we are concerned that your expectations highlight a serious lack of understanding (in our view) of the status quo among the eco systems of smaller Fixed Voice CPs (but in some cases larger CPs as well) based on topologies and how customers consume PECS that are not vertically integrated CPs. We should emphasise we are not advocating that CPs be mostly or completely internet based, but we know a large portion of the PECS and PECNs are by volume of participants. Again, we

²² https://www.ofcom.org.uk/__data/assets/pdf_file/0030/208587/gamma.pdf - paragraph 26

²³ https://www.ofcom.org.uk/__data/assets/pdf_file/0024/208590/simwood.pdf - page 4

²⁴ https://www.ofcom.org.uk/__data/assets/pdf_file/0029/216794/statement-2021-26-wholesale-voice-markets-review.pdf - Section 9.26 -

²⁵ https://www.ofcom.org.uk/__data/assets/pdf_file/0031/247486/statement-improving-accuracy-CLI-data.pdf

point to the example of SIP Trunking as a major B2B service that typically operates over a public internet connection.

Furthermore, reinforcing our point regarding knowledge gaps of the fixed voice sector. In 4.114 of the consultation and 4.2.4 of the guidance you refer to GSMA/NICC standards that imply interconnect should not be over the internet. The GSMA in our view is typically for mobile operators (and related ecosystems/industries). If you exclude Ofcom, the GSMA only has 5 operator members in the United Kingdom who are CPs²⁶ (a recent survey by DCMS highlights several thousand CPs). Therefore, referencing standards and applying them as fact as if they apply to fixed voice CPs is in our view misleading. Furthermore, the GSMA standard being referred to are completely out of reach of most CPs unless (from our understanding) we pay for access to read the standard.

In addition, when reviewing the latest ND1643²⁷ guidelines in our view it can be argued it does not prohibit internet interconnection. We see this in two area's:

1. section 1.1 referring to interconnection is directly or indirectly physical and logical or a combination – Public Internet Interconnection is somewhat indirectly as addressing space is being utilised across some kind of network rather than 2 physical SBCs sharing a cable. This is indirect in our view and can be a closed or open network (e.g. 2 LANs connecting together or over a wider WAN respectively).
2. control 32 where it states *"Except where direct communications are required, CP should maintain logical separation of the interconnect partner from other external sources (e.g. other interconnects, the Internet). Filters, SIP proxies, firewalls, vLANs or other technology may be used to maintain this separation."* - In our view this implies that interconnection via internet is acceptable because a) it says "should" maintain logical separation (not "must") b) interconnects (regardless if they traverse partly, in whole or not at all over the public internet) can and are typically logically separated utilising firewalls to only allow certain IPs through (i.e. that of the other interconnection switch) which is known as IP Authentication and on rare occasions credential authentication and c) generally SIP proxies or the SBCs themselves are used to separate and identify traffic from one source to another (which in our view is logically and algorithmically separated).

We appreciate that the original few versions of ND1643 whereby in our view did give the impression that interconnection should not be via public internet, although in recent iterations in our view does not exclude it. Furthermore, we note that at the time of when the consultation and guidance was originally published, V1.1.1 (2009) which was footnote 34 does give the impression internet based interconnection is not permitted²⁸.

²⁶ <https://www.gsma.com/get-involved/gsma-membership/our-members/>

²⁷ <https://niccstandards.org.uk/wp-content/uploads/2023/06/ND1643V5.1.1.pdf>

²⁸ <https://niccstandards.org.uk/wp-content/uploads/2019/03/ND1643-Minimum-Security-Standards-v1-1-1.pdf>

However as referenced above, the most recent version V5.1.1 (2017) in our view does not exclude internet based interconnection.

In addition we note in your statement response of the 2017 Consultation: Review of Security Guidance that you summarise responses in 2.18 stating “*Several CPs requested confirmation that ND1643 was still required as a standard by Ofcom and some questioned whether it was still relevant.*”²⁹. We appreciate this is prior to ND1634 going from certification to guidance.

We are open to being wrong and having misunderstood ND1643 ourselves, but genuinely do not think we are. We would welcome clarification on explicitly why and where you feel ND1643 implies interconnection should be non-internet.

Potential Solutions

Given the large eco system of CPs that are internet connection only and do not operate their own colocation setup (therefore adopting a non-internet interconnection maybe cost prohibitive or outside the technical competency of much smaller CPs) we believe there needs to be recognition of this along with the wider value they provide and the niche areas that maybe served by them.

We therefore feel that there needs to be a middle ground among security requirements that are not negatively market impacting in a material effective way. Many smaller CPs are micro entities and therefore on the whole maybe directly exempt from much of the Regulation and Code of Practice (although could still be enforced in parts due to contractual requirements with other CP suppliers). Our belief is the proposal around interconnect goes far beyond the Regulation and Code of Practice. There is also a real prospect (in our view) that this change could terminally impact the livelihoods of many smaller CPs who only have a handful of individuals behind them. Therefore, we believe Ofcom do owe these smaller CPs an extra duty of care.

Therefore, incorporating the current policy frameworks, we think will appease some of the concerns. It is our view Regulation 4(5) (encryption) will filter down to smaller CPs from larger CPs implementing their requirements. We also believe the recent CLI changes (which we feel is already having a positive impact) will go some way to overcoming some of the concerns raised by other CPs historically. We also see benefits under certain circumstance to enable medium to larger CPs to have a hybrid approach for enhanced resilience implementing a non-internet and internet interconnection model.

In summary, we feel that public internet interconnections should be permitted whereby the overall voice volume on the interconnect is expected to be < 5,000,000 minutes per month or 500 concurrent calls (which ever limit is higher) and this limit is per interconnected switches. We would also like to see this brought in at the same time as the requirements set out in Signalling Plane 4 in the Code of Practice for 31st March

²⁹ https://www.ofcom.org.uk/__data/assets/pdf_file/0028/108856/Statement-review-security-guidance.pdf

2028¹⁶. We feel this date would make it administratively simpler and is the date by which interconnections should be encrypted (therefore any interconnects that need to be migrated are potentially all done at the same time to ease administration and reduce roadmap fatigue). We also feel this is a good mix in balancing risk and not effecting the eco systems of smaller CPs and provides a roadmap for growing CPs at a point which they will need to consider enhancing their infrastructure and interconnection resilience which should in itself enhance the overall security by design requirements.

Finally, as many fixed voice CPs do provide the majority (if not all of their PECS) via the public internet, then in our view the focus should be on how to mitigate the risk of security compromise due to the risks of being public internet facing and the type of service being provided. This could include CPs investigating and implementing various strategies which could include (list is non-exhaustive):

- enhanced firewalling from only known and trusted sources
- utilising middleware topologies that authenticate and can absorb a large amount of requests (e.g. DDoS).
- Have plans in place in the event of external DDoS
- Geo blocking (i.e. only traffic within the UK or UK regions can access such service)

We would also like to see Ofcom proactively and constructively engage more with smaller fixed voice CPs in the sector.

Answers to Ofcom's 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?

For the most part we believe the suggestions are appropriate and proportionate. However, there are elements we have concerns with, as mentioned above and below.

In 4.17 as highlighted previously, larger CPs on the interconnection may dictate what may be appropriate and proportionate from their perspective, but not the smaller CP putting undue operational and economic burden where those both respective CPs need to interface.

In our view in 4.36 an internet interconnection actually increases resilience as the path to the other CP increases substantially given there would most likely be multiple ways a voice packet of data could route (including through multiple transits, and potentially Internet Exchange connectivity) into that CP and typically an internet interconnection model does allow for a broad spectrum of geographical resilience meaning there's less risk involved should there be a facility failure allowing smaller CPs to increase their resilience and diversity at lower costs.

It would also be helpful if there was a small section within the guidance that explained CPs should consider if any of their sites should be added to the protected site list as part of the electrical supply emergency code. For example, sites that host core elements of

the CPs network that may be critical in handling and processing emergency calls for that CP. Under the current guidance many CPs (including smaller CPs) who provide PECS over the internet service customers nationally. Therefore, from our interpretation, there maybe scope to be able to request (in conjunction with their data centre provider) to be added to the protected site list³⁰.

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

Yes we believe the suggestions are 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?

Yes, we think they are reasonable, appropriate and proportionate. However, following on from the points raised in 4.95 and 4.103-4.104, we feel it is important to highlight where CPs may procure connectivity from another CP for their OOB connection (should their network fail), it is important to conduct due diligence to check that the OOB is topology separate from that of the procuring CP to avoid any single or common points of failure. We'd also request guidance on whether this procurement will fall out of scope of Regulation 7(4)(a)(ii)³¹?

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

On the most part we agree, except for points 4.110 and 4.114 as previously discussed. In 4.110 we do agree with CPs needing to make provisions for fast and scalable failure detection and failover.

It is important to highlight that the points raised between 4.111 and 4.118 are specific depending upon the type of fixed voice service (e.g. digital phone line or SIP Trunk) being provided and how the physical link to the customer premises is being provided (i.e. is the CP vertically integrated and therefore has control over voice prioritisation or has the customer sourced an internet connection from one provider and a fixed voice line service from another?).

It is worth considering that where the connection is to a business that has their own setup (e.g. in the provision of SIP Trunking) then in our view it should be the responsibility of the business to make sure their internal network setup prioritises voice traffic, since their setup will be more bespoke and more likely to have higher quality internet lines such as leased lines. Equally, in the scenario of consumers, where different providers are being used (i.e. CP A is the ISP and CP B provides the digital voice line to interface with a customer or CP providing an ATA or SIP Dect Phone etc.), it is usually the consumers

³⁰ <https://assets.publishing.service.gov.uk/media/60ccc3698fa8f57cef61fccd/esecc-guidance.pdf> - Table 1

³¹ <https://www.legislation.gov.uk/ukxi/2022/933/regulation/7/made>

responsibility to make sure their internet connection meets minimum standards as the voice line provider would practically have little to no view or input on this.

Expanding on the previous paragraph further, it is also worth considering whether ISPs should be required to automatically provide routers that priorities voice packets (similar to password requirements³²). Given voice standards are well known and given many of the domestic routers in use can already do a form of packet prioritising (i.e. just a configuration option that requires enabling), then it maybe worth while exploring this concept further so consumers do not need to modify settings themselves within the router to prioritise voice packets.

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?

Yes, we believe the suggestions are appropriate and proportionate.

CFI Question 1-10

We are not a Mobile CP and therefore our knowledge is limited in this respect although we feel that the 1 hour minimum target is not ambitious enough given how the PSTN is being shut down and likely more people will be relying on their mobile phones in the event of a power outage (especially for emergency calls) as reinforced by 2.19 and 5.11 of the consultation. Therefore, they would be expecting their mobile phone reception to last for the majority of a power cut. This concern is highlighted in your Annex 2 (table 1) power outage data which suggests more than 30% of all power outages were over 1 hour. Therefore, based on this we believe that the target should be 2 hours so approx. 80% of power outages would be covered.

Furthermore, during a power outage, we would expect that voice and SMS services at a minimum are available so emergency calls can be made, vulnerable individuals can still be contacted and where there are more serious events that occur (such as power outages related to storms etc) then those involved in assistance can arrange appropriate support.

Finally, where it is expected that a power outage will impact a larger proportion of the population in a more densely populated area or a smaller population in a more rural area, if a power outage was expected to last more than 12 hours, then provisions should be made on how mobile operators can keep their cell sites operational (such as investigating the feasibility of an option for an on-call portable generator to be deployed at short notice).

³² <https://www.legislation.gov.uk/ukxi/2023/1007/contents/made>