Question 1 – What are your views on emerging and potential future security and availability risks and whether they should be addressed in the revised guidance?

Yes, they should certainly be addressed in the guidance. I would challenge the quality of the Detica report as a primary source of input. Firstly the report lacks any supporting evidence and is anecdotal and hearsay. For example the reference to Army personnel almost exclusively providing the skilled workforce is incorrect. Armed Forces Service careers are short lived with full term serviceman leaving the service after 22 years. Too young for retirement many service personnel pursue challenging and well paid careers and Networking is an attractive choice. Mobile Network Engineering is of particular interest as candidates can attend a short resettlement course upon leaving the service and become qualified and be working in the field within a few weeks. Due to the demanding nature of these roles they are not very attractive to the young emerging workforce. It has nothing to do with Army providing the training as it does not (with the exception of specialist trades in the Royal Signals). As long as we have Armed Forces in the UK there will be a steady stream of skilled engineers entering the telecommunications industry regardless of what training the Army provides them with during service.

In my experience the risks to availability are not new and have existed for at least a decade, all that has changed is that the gap is increasing as technology advances and there is greater public awareness but the risks are fundamentally unchanged. These are a small number of broad risks that that been protracted here into a larger number of detailed risks in the Detica report. As the gap is widening it is concerning that we are not applying lessons learned from previous serious incidents such as the service tunnel fire in Manchester in 2004 where much of the North of England lost telephone, internet and private WAN service. This highlighted that despite customers having resiliency in contracts with CPs (dual bearers to separate exchanges) that single points of failure still existed and has devastating consequences when incidents like this occur. Big CPs like BT have always been obscure to customers about the infrastructure in the service "cloud" and this still remains the case today (even in Government and large commercial contracts) yet little seems to be done about this and needs addressing by Ofcom in this review.

The Detica report does not address confidentiality or integrity at all and only deals with availability. If a criminal is able to break into an unmanned facility and steal equipment then what is to stop a criminal organisation or foreign intelligence agency breaking into a facility and tapping equipment so that they can wholesale steal and/or modify customer information covertly and indefinitely? Risks of this nature and context are not mentioned anywhere in the documentation however the Detica report by implication suggests this is a serious risk.

Question 2 – In relation to the obligations to manage general security risks, how should our guidance be revised to reflect issues such as ENISA's Guidelines on security controls, supply chain management, the use of 3rd party data centres and applicability to smaller CPs?

The ENISA guidelines are generic enough to be applied to any size CP organisation. A term widely used in information security is "proportionately" however I did not notice this term used anywhere in any of the documentation. Security is scalable the same way networks are. Additionally security is integral to all modern ICT technologies so the size of the CP should not really matter. If a CP is operating a global network or simply hosting a few websites if they have the expertise to deliver a technology in the first place then they should also have the knowledge to understand how to do so securely. Certainly if they are formally trained/certified then security awareness for the technical discipline will be likely.

Enforcement of the ENISA guidelines is largely subjective so I would consider incorporating terms such as "Due Care", "due diligence", and "prudency" into the guidance. For example It would be very difficult for a CP however small to prove due care and prudency if they did not install firewalls at the network boundaries or install anti-malware software in their data centres when even an average non-technical home internet user may be prudent enough to install anti-virus software on their PC and understands that their broadband router has a simple firewall installed out of the box. Exactly the same principles and controls but at opposite ends of the scale in terms of proportion and failure to do in both cases would be clearly negligent.

In respect of third parties, legal responsibilities and liability should be clearer and that in terms of end customers the book stops with the CP providing the end service. CPs should be required to ensure that they have adequate protection from incidents caused by third parties by ensuring that they are contractually covered and have contingency plans (business and technical).

The ENISA guidelines themselves are somewhat patchy. The guidelines describe three levels of control, Basic, industry standard and State of the Art however when you read the definitions in the tables this is not the case. The level of security could actually be exactly the same for each level in practical terms and to move from Basic to Industry Standard simply requires the CP to capture the controls they have in place in written policy and to move to the highest level of State of the Art only requires the CP to review the controls and policies from time to time. In essence, there could be no difference in the level of actual security between a CP operating at basic level and another operating at state of the art giving a clouded view of the level of security applied by the CP

Question 3 – How best can risks to end users be considered by CPs and appropriate security information be made available?

As suggested in the guidance there is no one size fits all for consideration of risks to end users as each CP would need to conduct risk assessments in context to their own operations, services provided and customers which will vary from one CP to another.

Assuming that there was a standard/guidance to follow (such as ENISA) then perhaps it would be a good idea for CPs to have the capability to be measured and publish the results in a competitive manner. The introduction of Ofsted grading's for Schools, Colleges and child care premises has had a significant impact on customer choice and selection which drives the standard up across the board. In private organisations such as day care nurseries those that fail to meet the standards expected will go out of business and those with high standards will thrive. A similar scheme could be employed in the CP industry. This would need to be voluntary and inspections could be funded by the CP and carried out by third party SMEs contracted by Ofcom. The CPs grading and brief summary can be published publically by Ofcom. Broadband performance metrics published by Ofcom have proved invaluable to the general public but as the public become more security aware year by year then I believe a system that includes security would prove equally valuable in future years. One could argue that smaller CPs would not have the resources to participate in such a scheme however proportion again is key. Small organisation could mean a smaller, therefore cheaper and less complex audit requirement.

It is worth to note that in terms of consumer choice there may seemingly be a large selection of CPs for consumers to choose from but in fact in any given geographic location there may actually be only one large CP operating the infrastructure with the rest being resellers of wholesale service. With this in mind any security information made available to customers may not give an accurate overall view of security for the services of interest.

Question 4 – Should Ofcom consider additional guidance in relation to network availability and the provision of related consumer information?

Yes, I believe there should be a legal requirement for CPs to publish availability information in real or near-real time on publically accessible medium for example the company websites. This should not be the direct responsibility of Ofcom but should be monitored by Ofcom. In many cases, smaller CPs are very good at this but some of the largest CPs are very bad and in fact will lie about outages or fob customers off altogether when things go bad. Also, there should be tighter legislation about claims of availability. CPs may claim 99.9% uptime on the public website but this in fact could mean anything from end to end service availability to when the CEO last slept. All outages that affect service to customers (including degradation of service) should be published and made publically available and claims of uptime independently validated if dubious.

Question 5 – Would it be useful to clarify our expectations around reporting in the case of wholesale and “over the top” arrangements, and the need for CPs to maintain sufficient fault monitoring?

Yes, this is important to understand the impact from dependencies. For example there may be several incidents reported from smaller CP's that the smaller CPs may regard as critical to their business but the incident may have its root cause in an incident considered minor at a large CP that has provided

the wholesale service to the smaller ones. There should be a duty on wholesale CPs to report faults immediately to their customers (smaller CPs) rather than the opposite way around as the reports suggest is the case today i.e. be proactive rather than reactive.

Question 6 – What are your views on the appropriate thresholds for reporting incidents affecting customers of smaller CPs, mobile networks, data services and services suffering partial failures?

The thresholds seem straightforward and appropriate however without further insight into the experience so far of Ofcom it is difficult to comment. It should be noted that there are circumstances where additional reporting may be desirable above and beyond the thresholds. For example communication services that have health and safety implications that are not part of the usual 999 services. Some examples are home safety networks that are linked to the households of vulnerable people, environment monitoring networks in high safety risk areas, security service secure communications networks, security operations centres etc. Incidents affecting these areas may be under reporting thresholds but have significantly more serious impact to public well-being and safety.

Expanding on this latter point, the threshold system makes no allowances for the criticality of CP services provided. Some of the example quoted above may be regarded as critical however many of these service providers would fall into the small CP bracket as niche providers and may be reliant on infrastructure provided by larger CPs. In terms of WAN conveyance infrastructure, there are only a very small number of CPs in the UK and the majority of CPs providing communication services of one form or another will be letting or reselling the infrastructure from these minority large CPs. It should be considered that a small number of large CPs are perhaps part of the UKs critical national infrastructure.

Ofcom should be empowered to request more detailed reporting beyond the thresholds at their sole discretion if it is thought that a particular application/service warrants it.

Question 7 – What are your views on revising the current process for reporting significant incidents?

Considering in many cases reporting incidents to Ofcom could be sensitive in a number of ways then secure reporting should be the norm rather than using unsecured email. It should not be difficult to setup a secure form on the Ofcom website or provide a secure file transfer. The current process seems a little unprofessional and my view would be (as a CP) that if Ofcom as the UK Government Regulator cannot make a little investment in security then why should they.

General Comments

1. If I recall, the review paper alluded to their being only one area dealing with data networks and seven against traditional fixed line telephony in the current policy. In my view, fixed line telephony still only has a place in many UK households because it is pre-requisite for broadband and if this were not the case then over time it would become obsolete altogether. Inclusive minutes in cheap mobile phone contracts (and pay as you go) means that fixed line telephone services are on the decline. Many CPs recognise this, including mobile telephony operators and home internet contracts are now available where effectively the BT telephone line is bought at a reduced cost by the CP and offered free of charge to the end customer effectively as part of a broadband package. The customer does not make calls from the landline (as they attract a high tariff) and uses their mobile for phone calls then this is a cost effective approach. It is essential to be ahead of the game and monitor this trend.

2. In UK society, data networks are an essential part of life in Government, business and at home and should no longer be considered as a "nice to have" and as mentioned in a previous comment perhaps form part of the Critical National Infrastructure. For example for some people the loss of internet or upstream network services could be devastating to their lives. We are dependent on networks and the internet for banking, grocery shopping, utilities such as gas, electric and water, travel, communicating with distant family and friends and so much more. A missed rent payment paid by online banking could see families out on the street. With the introduction of the "Digital By Default" GDS policy we are seeing welfare services that affect millions of UK households moving online, Universal Credits, Personal Independence Payment and so on. There is a need to be seen to be taking this a lot more seriously then we seem to be. Many organisations maintain their legacy paper and POTS based services alongside their digital and online services but would they be able to continue business operations to effective capacity should their network services become unavailable?

3. There is a lot of reference to CPs having outdated documentation and lack of technical and historical knowledge within the CPs making incident resolution difficult due to the lack of detailed topography and configuration management information This is a serious concern and is not limited to commercial environments but Government environments also. I believe there is a need for stronger legislation in this area. Private companies are required by law to keep and retain certain documents (for example financial information, medical records etc.) and this information is auditable. I think there needs to be similar legislation introduced for CPs to maintain documentation for their networks and services. In my opinion CPs should be required in law to document network topology and configuration management information and keep this up to date. Like financial reporting, sufficient grace periods should be allowed for updating following change (12 months perhaps) then Ofcom should audit/inspect targeted organisations within

whatever means and resources are or become available to them and impose penalties for non-compliance. This could be a useful deterrent for non-compliance.

4. Although there is a loose reference to the UK Cyber Security Strategy there does not seem to be any alignment with the strategy. The Cyber security strategy offers lots of preamble and context to the threat landscape and is warmly presented creating a feeling of "all being in it together" which is aligned with wider UK Government ICT strategies and reforms whereas the Ofcom guidance is very cold and wooden. Various government departments seem to be leading on certain areas of security but the Ofcom guidance seems disjointed, out of date and out of step with everyone else. I strongly feel that a revision of the guidance should be presented with a similar feel to other Government guidance and should also be inclusive of, or reference the work that the Cyber Security Program, BIS and everyone else is doing and be clearer what the part Ofcom plays in it. Currently it may seem contradictory in that on the one hand some Government organisations are asking for voluntary participation and on the other hand other Government departments are mandating it. While it may be obvious to some that Ofcom is concerned specifically with regulating the communications industry and that network security goes beyond cyber security this will not be blatantly obvious to all. Many see cyber security as another name for security generally and that all Government departments are one and the same.

5. The Ofcom material only seems to be concerned with Availability of CP services and does not seem to consider Confidentiality and Integrity (from the CIA triad) at all. It could have been the case that this is intentional and out of scope of Ofcom coverage however it is clear that one of the main drivers for the revision of the Communications Act 2003 is European Legislation which is inclusive (albeit very patchy) with confidentiality. The ENISA documentation is confusing in that it incorrectly describes Availability as Integrity. This is further confused by the footnote about the use of this terminology but this is also incorrect. Integrity (in an information security context) is about data/information not being tampered with maliciously or modified inadvertently from non-malicious means and not as the footnote describes. Considering this, the Ofcom guidance addresses Availability only, ENISA deals with confidentiality and neither organisation addresses integrity (in a security context).

6. As suggested in several Government papers, The internet promotes freedom of information and speech like never seen before in history however some things that were historically considered not to made common knowledge (in the public's best interest) are unavoidably now in the public domain for all to see. Some examples being "spy next door" headlines, Government information leaks, eavesdropping scandals, industrial espionage and wholesale fraud and identity theft. This is no longer the stuff of John Le Carre novels but is known to be

reality by the UK general public. I personally believe that this has played some part in the production of the Cyber Strategies appearing from Governments across the world (UK included) but in the UK this is falsely being presented as something new when in fact some of these risks have existed for decades (and only tells half the story). The big thing that has changed is that the proliferation of digital communications networks and the internet have made it so much easier for criminals and foreign agents to conduct their activities and on a much larger scale. Ask a member of the public who is OCSIA, CESG or even CPNI is and they probably will have no idea. Ask them who Ofcom is however and they will probably give a fairy accurate description. Ofcom is the UK Government face of the communications industry and a layperson would likely assume that it is Ofcom that is ensuring that our national security, economic health and public well-being are being maintained through regulation of the communications industry (where appropriate) but the guidance does not seem to imply any of this. The current guidance is analogous to punishing a child for reaching for a hot pan on the stove but failing to educate the child and tell them that the pan is hot and it will burn them!

7. Large CPs and some private organisations (such as List X companies) may well have direct relationships with the organisations mentioned above (and others such as MI5/6)) and be well informed about the threats but what about the smaller CPs, the organisations that they effect and of course the general public? I would have assumed that Ofcom would have a role (perhaps lead) in all of this but this does not seem to be case. Truth be told, the organised crime and state sponsored activity is made easier because it is easy to hide and cover your tracks when using the digital communications and some of this could be reduced by more effective control and regulation in the communications industry. For example in the case of a bogus website (with a URL similar to a leading brand name) the criminal will have multiple instances of the website hosted with a number of different hosting companies, the DNS will be registered with someone else, the domain name registration somewhere else again, and the criminals will conduct their activity from somewhere else again, probably from a compromised host in another country and will operate via an anonymous proxy service. The effort and expense for the targeted company to get the bogus site shut down can be crippling. If they contact the hosting company at best the host will shut the site down but the criminal will (via DNS) simply activate one of the mirrors, at worst the hosting company will demand a court order and weeks later shuts the site down for it still to be moved somewhere else. In the case of more sinister activity such as state sponsored persistent attacks it may be known to UK security services that these attacks are occurring over a prolonged period time. Where the attacks are occurring from and where compromised information is being sent is sometimes known and recorded on "blacklists" yet there is no legislation (that I am aware of) that ensures that this activity is blocked at network boundaries by the CPs or that the blacklists are even shared unless it becomes an issue

of national security. My point being that there needs to clearer guidance, perhaps a mandatory requirement for CPs to block and prevent illegal activity without unnecessary delay as an act of due diligence and that government security departments need to be more transparent and share what they know with the CPs, the wider public and industry and where appropriate guide legislation to be enforced by Ofcom or other appropriate bodies.