TELEFÓNICA UK LIMITED RESPONSE TO:

"Review of Security Guidance: Consultation on updating Ofcom's guidance on security requirements in sections 105A to D of the Communications Act 2003"

NON-CONFIDENTIAL VERSION

September 2017

I. INTRODUCTION

1. Telefónica UK Limited ("Telefónica") welcomes the opportunity to respond to Ofcom's consultation on updating its guidance on security requirements in sections 105A to D of the Communication Act 2003.[1]

2. Telefónica takes its responsibilities in relation to security extremely seriously. Telefónica holds security certification such as ISO 27001 for all customer and employee data; ISO 22301 for all activities; CAS-T for mobile voice and data; ND 1643 (Minimum Security Standard); and the Cyber Essentials Plus Assurance, for which we are committed to having externally reviewed by BSI annually, in line with the guidance provided by Cyber Essentials.

3. Telefónica is a leading member of the Electronic Communications Resilience & Response Group (EC-RRG) and was the author of the first iteration of the National Emergency Alert for Telecoms (NEAT) protocol designed to bring Industry and Government together in response to major incidents or emergencies and aimed at mitigating or reducing service impacts to the UK.

4. Telefónica is also an active member of the Telecommunications Industry Security Advisory Council (TISAC), a participant in the Cyber Security Information Sharing Partnership (CiSP) and has for a number of years, followed the CESG/Cabinet Office 10 Steps to Cyber Security Framework.

5. In addition to the above, Telefónica is actively engaged on security matters with numerous industry peers, law enforcement and government agencies and has active and ongoing relationships with CESG, NCA, CERT UK, CPNI, NSIE, and FIRST.

6. Telefónica has also created a CERT (Computer Emergency Response Team) that works closely with CERT UK. Resource in this team and other security areas enables us to enhance, even further, our response to ever changing, and increasing, cyber threats.

[1] https://www.ofcom.org.uk/__data/assets/pdf_file/0024/103596/consultation-review-security-guidelines.pdf

7. We agree with Ofcom that it is important for Communications Providers to take appropriate steps to manage security risks including ensuring that risk management, governance and ownership is in place up to, and including, Board level. We also support Ofcom's view that it is appropriate to look at existing detailed guidance and best practice when assessing the area of security, for example The Government's "10 Steps to Cyber Security" and Cyber Essentials.

8. We very much welcome Ofcom's engagement with industry on this subject as co-operation, collaboration and communication is a key part of ensuring the highest levels of preparedness and responsiveness to security threats.

II. SECURITY & AVAILABILITY (s105A)

Cybersecurity

9. Please see the information and comments we have provided in the Introduction section above in relation to our position on Cybersecurity, including risk management, controls, governance and security standards and best practice.

Single Points of Failure

10. We note Ofcom's comments in relation to single points of failure and agree that the extent to which avoiding single points of failure is reasonably possible, will vary at different points in the network. We believe that examples of a relevant consideration should also include an individual base station i.e. a single mobile site.

11. However, we disagree with the stated definition of a single point of failure as being "instances in which the network relies on significant amounts of traffic passing over a single route, a single point of handover, or on routing through a single location, thereby leaving the service vulnerable to a single point of failure". This definition actually describes significant traffic loading, and does not describe a single point of failure. Rather a single point of failure would require **all** traffic to pass over a single route, a single point of handover, or on routing through a single location.

Flood and Power Resilience

12. Ensuring a high level of resilience across our network is already very strongly driven by our desire to provide our customers with the best possible service, maintain our excellent customer satisfaction levels and protect our reputation and brand. These important drivers, along with the fiercely competitive nature of the UK mobile market, ensures that we are already fully incentivised to provide a high level of resilience in our network. As such, we do not think that there is a case for Regulatory intervention to attempt to force operators to provide greater resilience.

13. In relation to the specific risk of flooding, we note Ofcom's comments that CPs should still consider whether additional measures are required, even where sites are identified as being at a lower risk of flooding. We believe that such consideration is already carried out through our review of service outages in the form of our Post Incident Review (PIR) process, which generates a formal assessment of service risks and mitigations which forms the basis for any further actions or measures that may be deemed appropriate to take to reduce the risk of a re-occurrence of the service outage.

III. INCIDENT REPORTING (s105B)

Mobile Reporting

14. Telefónica has made it a clear priority to put its customers at the heart of its decision making and activities. With this forefront in our mind, when we experience significant network incidents that affects the service that we provide to our customers, we devote our efforts and resources toward trying to fix things as quickly as possible with the minimum amount disruption and to communicating to our customers. As such, whilst we appreciate the importance and benefit to Ofcom of the existing reporting requirements, we are concerned that some of the proposals to change the reporting thresholds and requirements, will result in an overly burdensome process that could divert resources away from the task at hand of service restoration for our customers.

15. We note Ofcom's comment that the clear majority of reported incidents are examples of routine problems which inevitably occur when running complex networks in the real world. However we are concerned that Ofcom's proposal to amend the thresholds for mobile reporting will create an unnecessary reporting burden as the thresholds proposed are likely to mean a far greater number of reports being generated and sent about routine problems, possibly on an almost daily basis,

we would question the benefit gained by Ofcom receiving such a volume of reports on issues which are considered routine.

Mobile Reporting Thresholds

16. We disagree with the proposal to report the loss of a single technology for 25 or more sites with a minimum duration of 2 hours. The proposed measure does not account for the fact that customers have the ability to switch to other technology layers in the event that one layer loses service. We strongly suggest that the threshold is amended to reflect the loss of each *service*, for example total loss of voice or total loss of data, such incidents are far more likely to have an impact on customers, whereas the proposed single technology threshold could result in minimal or no impact to customers at all. We believe that it is more appropriate to focus reporting on incidents which have a greater impact to consumers.

17. We also disagree with the proposal for the minimum duration to be set at 2 hours. [✂]. We suggest that the minimum duration is set to 4 hours which reflects a more realistic and practical level.

18. We assume that when Ofcom refers to 25 sites, it is referring specifically to adjacent sites and not ones that are geographically unconnected, we would welcome clarity on this in the final guidance.

19. The proposed reporting thresholds for customers in rural areas are problematic. Whilst it is entirely sensible that it is based on total loss of a *service* (and not a *technology layer*) as explained above, the proposal to report for a single site that is in an area classed as rural (according to a classification system) is likely to result in a significant reporting burden. It is not clear how we are able to identify whether a particular affected site falls within the rural classification without carrying out an extensive amount of work to determine this. We suggest that the proposed threshold is instead amended to a set of pre-defined and agreed, remote rural locations in order to avoid an unnecessary burden in identifying whether a site is classified as rural or not. This would also avoid the likely scenario (under the proposed threshold) of a large number of single site reports having to be generated and sent which would serve little purpose as they would again reflect the type of routine problems that inevitably occur as a result of running a very large number of sites as part of a complex network.

20. For such rural sites, we do not agree that such incidents should be reported regardless of whether emergency roaming would have been available, which is a change to the current guidance. We would appreciate further explanation from Ofcom on this proposed change to the guidance in order to understand the basis for the change.

21. We understand Ofcom's desire to achieve a more consistent level of reporting from mobile operators and receive a significant and sustained increase in reporting from those mobile operators which are currently reporting infrequently, whilst avoiding a reporting process which is unduly complex and burdensome. However, we do not believe that the proposed changes will result in the desired outcome that Ofcom is hoping to achieve.

Reporting Affected Sites

22. We disagree with the proposal to provide a full list of affected sites in relation to mobile incidents. This will create an unnecessary burden, furthermore such a level of data is not required in the aggregated ENISA report under Article 13 of the Framework Directive. This unnecessary burden can be avoided by instead requiring mobile operators to provide a simple narrative statement, or a basic map snapshot, of the general geographic area which will provide sufficient clarity to identify the area affected by the incident.

Cyber Incident Reporting

23. We disagree with the proposal to report cyber-attacks that meet *any* of the qualitative criteria for reportable incidents. Specifically, we do not agree with the criteria which covers where such incidents have been reported to other Government agencies or departments. For example, where we would report an incident to ICO, under the Privacy and Electronic Communications Regulations (PECR), i.e. an incident that does not impact upon our core services to customers (i.e. it does not affect voice or data), we would not expect there to also be an obligation to report that to another Regulator.

24/7 reporting process for urgent incidents

24. We understand Ofcom's desire to be informed about major incidents and those which attract national mainstream media attention or political interest. We note what Ofcom says in relation to having received enquiries or seen media reports about very serious incidents before it has been notified by the CP involved. However, with the rise in popularity of social media and the nature of its immediacy, along with rolling news availability, information now enters the public domain far more quickly, often within minutes, therefore it is inevitable that some incidents may be known about through such media before they are formally notified to Ofcom. This would still be the case even if a reporting obligation was set to just 1 hour, or even less. As such, setting a reporting threshold of 3 hours is unlikely to mean that it will *always* be notified before it may have received an enquiry, or seen media reports about the incident.

25. We would appreciate further clarity from Ofcom with regard to out of hours reporting, for example whether Ofcom would expect to be notified of a major incident which occurred at 1am on a Sunday morning, through receiving a phone call

between 1am and 4am, thus adhering to the 3 hour reporting proposal. We would be happy to discuss this further with Ofcom to agree on a viable process and we also note Ofcom's intention to share the urgent reporting contact number directly with CPs.

Calculating the number of affected users

26. Calculating the impact of service incidents on customers is a highly complex exercise, with no single system having the ability to provide a robust accurate measure. [✂]. Such calculations are somewhat crude as they are performed using a script, however, they are service-based (i.e. voice, data) and not individual technology based (i.e. 2G, 3G, 4G).

27. Ofcom's proposed methodology of technology-based reporting and calculation is problematic as it is not compatible with our data capture and reporting. Furthermore it does not consider the inherent resilience benefits of a multi-layer network i.e. the offload from one technology layer to another e.g. 4G to 3G; 4G to 2G or the use Wi-Fi calling which is now increasingly available to more and more customers.

28. Furthermore, the nature of a mobile service means that customers will appear on more than one site and as such, could be unaffected in practice, as they are moving from the affected site onto another which is not experiencing a loss of service.

29. It is also difficult to establish the number of customers typically connected to the network via each site as we record *events* rather than *users*; for example ten calls on a site could be generated by between one and ten customers, so approximating the number of customers is likely to be far from accurate and potentially, misleading.

30. We believe that the proposed method is impractical and overly-burdensome due to the lack of counting capability in the parts of the network being indicated i.e. at the individual mobile site level. This combined with Ofcom's proposal to report single site outages in rural areas raises significant concerns for us.

31. While we understand and appreciate what Ofcom are looking to achieve (i.e. consistency in reporting the scale of impacts), it is apparent to us that the proposed methodology has many flaws and complexities. Furthermore, considering the proposed method in isolation could be unhelpful as this does not provide sufficient insight into the methods likely to be used by other MNOs to derive their impact figures, nor the level of consistency that will be gained from adopting any or all of the proposed method of calculation.

32. Due to the complexity and the 'devil in the detail' in this area, we do not propose to outline each and every element and consideration in our response, instead we think

that it would be more beneficial to discuss this in person with Ofcom and share our current calculation method for Customer Lost Hours, go through the Ofcom proposed methodology, establish the pros and cons of both and consider other possible methodologies which may provide a more accurate picture and result in a more consistent set of reporting by mobile operators.

IV. **CONCLUSION**

33. As the proposals stand, we do not believe that they would fulfill Ofcom's objective of a more consistent level of reporting from mobile operators and a significant and sustained increase in reporting from those mobile operators which are currently reporting infrequently, whilst avoiding a reporting process which is unduly burdensome.

34. However, we think that there is an opportunity to share knowledge and exchange views, through face to face discussion, to help facilitate the establishment of a pragmatic, customer-focussed set of thresholds and a methodology that mobile operators can follow, which provides Ofcom with sufficient timely information in order to be fully informed and carry out its duties, whilst not placing an unnecessary or excessive burden on operators.

35. We look forward to engaging with Ofcom on this and we hope that the comments and suggestions that we have provided in our response will assist Ofcom in its consideration of updating the guidance in a way that will result in the achievement of Ofcom's objectives and will produce positive outcomes.