NON-CONFIDENTIAL

Verizon Enterprise Solutions response to Ofcom's Call for Inputs on updated guidance on network security

1. Verizon Enterprise Solutions ("Verizon") welcomes the opportunity to respond to Ofcom's Call for Inputs on updated guidance on network security (the "CFI").

2. Verizon is the global IT solutions partner to business and government. As part of Verizon Communications – a company with nearly $108 billion in annual revenue – Verizon serves 98 per cent of the Fortune 500. Verizon caters to large and medium business and government agencies and is connecting systems, machines, ideas and people around the world for altogether better outcomes.

3. In summary, while Ofcom rightly recognises that the industry and telecoms environment has evolved and moved on since it first issued guidance in this area in 2011, it should not rush to broaden the scope of activities potentially covered without carefully thinking through the implications for stakeholders, and weighing up the true costs and benefits. It should also recognise the cost and burden that may fall on stakeholders if it chooses to change the focus of its guidance or signal new preferences for assessing compliance. Finally it should allow flexibility in terms of incident reporting, and not require those with efficient established processes to change their systems, incurring more cost and burden, just for the sake of realising some perceived marginal benefit.

4. Ofcom needs to strike a suitable balance between providing clear guidance and regulatory certainty on the one hand, and avoiding prescriptive rules with little flexibility on the other. We would also strongly caution Ofcom against acting out of step with its European counterparts. As Ofcom rightly recognises, it is crucial to work towards a harmonised regime vis a vis other EU countries, given the increasingly interconnected and pan-European nature of communications. It is arguable that Ofcom's current guidance was introduced prematurely and/or without full appreciation of the wider European context, and as set out below it now appears that Ofcom is having to shift its policy position as a result.

Initial remarks

5. As a pan-European communications provider (CP), Verizon maintains a keen awareness of European legislation and regulation in each of the EU Member States. It is apparent that, in relation to this area of the Common Regulatory Framework (CRF), Ofcom is far more pro-active than most if not all of its European counterparts in terms of issuing guidance and setting expectations. Indeed it issued guidance months ahead of ENISA,

the EU “expert” body in this area. It has also clearly spent considerable time engaging with industry to ascertain the degree of compliance CP by CP. [✂].

6. Ofcom clearly feels that significant time and effort needs to be devoted to this area of responsibility, perhaps because these are new responsibilities where its level of knowledge and understanding is still relatively low. It is for exactly this reason that we would urge Ofcom to take a measured approach to this area, and to act in step with its counterparts. It should take the time to fully understand and describe to its stakeholders how other NRAs are approaching the matter before setting more guidance. It is unclear whether Ofcom has done this, or intends to, in advance of any formal consultation – but this is something that Verizon considers is essential to ensure a common framework which meets the needs of all stakeholders.

7. Verizon is concerned, given the past experience of the way this matter has been managed, that Ofcom may go too far and too fast towards adopting a position which is out of step with the rest of the EU. It is not helpful if one NRA decides to act far in advance of, or out of sync with, its counterparts. This is especially the case where ENISA is expected to provide harmonising guidance in the near future. We would urge Ofcom to wait until the revised ENISA guidance is issued, and take that into account (as well as the views of other NRAs) before issuing any consultation in this area. A little restraint in this regard now would, in our view, be hugely beneficial to all stakeholders, not least Ofcom in ensuring this matter will not need to be addressed again in the near future in order to harmonize requirements across the EU.

8. In terms of incident reporting we would also take the opportunity to reiterate the need for Ofcom to reflect the differences inherent between consumer and business oriented CPs. Verizon often acts as an intermediate carrier in a chain between originating and terminating parties. Moreover, as a business to business provider, we do not have contractual relationships with residential end-users of communication services. Therefore if we were to report an incident affecting our network, it may well be the case that Ofcom would receive one or more duplicate reports from other carriers up or down the chain. Such an arrangement would seem to be disproportionate and inefficient. It would also appear to leave Ofcom with the task of having to determine which reports concern essentially the same incident. [✂].

9. Under the heading “Regulatory focus to date”, paragraph 2.7, Ofcom describes its ongoing programme to investigate incidents that are reported or that it is otherwise made aware of. It is suggested by Ofcom that events are prioritised where they may provide information that can be shared with other CPs. Where Ofcom does not already disclose

such information, it might consider publishing details of the investigations, even if on an anonymous basis. This would help give CPs a greater understanding of the type of investigations Ofcom is carrying out, the number, general outcomes and any lessons learned which may help broader compliance.

10. Ofcom makes clear at paragraphs 3.1 – 3.3 that prior to 2011 it had little experience or involvement in the area of security and resilience. It suggests that this lack of previous experience was the driver for publishing guidance. This seems counter intuitive. Surely having little or no experience in a particular area is exactly the reason *not* to issue guidance prematurely, but rather to consult with all relevant stakeholders, including other EU NRAs, and build up a base level of knowledge and understanding first.

11. We would hope that since issuing its current guidance, Ofcom has come to realise both the complexity associated with imposing security standards in this area and also the very extensive security measures already taken by responsible CPs in order to protect their commercial interests and those of their customers. Many CPs inevitably take measures that would meet and exceed any reasonable NRA expectations in terms of security and resilience – especially those CPs (typically B2B providers) whose customers expect and rely on a high degree of security and network resilience.

12. While suggesting generic standards may make an external security audit or compliance check more straightforward, it does not necessarily do anything to improve security or increase resilience. It arguably serves only to increase costs and the regulatory burden for CPs, who may well meet or exceed minimum standards with their own internal controls. Ofcom should ensure that it does not cause some CPs to shoulder an undue burden or be placed at a financial disadvantage just because they choose to rely on their internal bespoke controls rather than seek external certification. In this respect Ofcom needs to be flexible about the type of evidence it will accept to demonstrate compliance, and look at the wider context of the type of customers and market a CP operates in. For example, the customers of a mass-market consumer CP may have a different view on security and resilience, relatively speaking, to the customers of a B2B CP who are typically government departments and large corporates. It should certainly not be the case that CPs feel compelled to spend money to certify their operations against external standards just because it makes it easier for the NRA to satisfy themselves that they are meeting generic minimum standards.

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?

13. We do not consider that Ofcom has made the case for widening the scope of the guidance to include potential new areas. Ofcom is the first to admit that it has little knowledge and experience in these areas, and it should now realise that it is unhelpful to issue guidance in such an unprepared state. Ofcom also makes the point that the Government is already investing in developing its own strategy in this area, so we would want to consider the outcome of this initiative before seeing any further additional guidance from the NRA. It is really important that when faced with these types of emerging issues, which may touch a number of competent authorities, those authorities work in a co-ordinated manner so the industry is not faced with multiple sources of guidance and possible initiatives which all face the same direction but in slightly different ways.

14. In any event Ofcom should not underestimate the seriousness with which responsible CPs take emerging threats such as cyber security. By introducing guidance, or setting out its views when it is not yet fully informed, will divert resources and attention away from tackling the issues for little gain. It should take sufficient time to fully consider the current approach taken across the industry before it looks to introduce additional guidance, however well-meaning it may be.

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?

15. In its original guidance Ofcom gave the strong impression that as far as section 105A is concerned, evidence of compliance could prima facie be demonstrated most easily by certification against the ISO27000 standard. While alternative evidence might suffice, it was clear that the ISO270xx standard was uppermost in Ofcom's thinking, and a strong preference. Ofcom said the following:

> *For demonstrating that basic security practices have been adequately undertaken many larger CPs are likely to be able to rely on their existing compliance with information security standards* ***such as the ISO27000 series***[1] *[emphasis added]*
>
> *Our preferred form for such evidence [that interconnecting CPs have protected themselves in the event that they do not seek certification against ND1643],would be external auditing against controls in other standards covering the same areas as those in ND1643, with* ***the most likely source being the ISO27000 series of standards****. Absent any suitable external verification, more detail will be required to allow Ofcom to satisfy itself that the organisation has taken sufficient steps to protect network*

[1] Paragraph 3.11

> *interconnections. If this cannot be readily obtained, it may be necessary to consider exercising our external auditing powers under Section 105C.*[2] *[emphasis added]*

16. Not only was ISO27000 apparently Ofcom's preferred option, but the text above implicitly suggests that absent certification against this standard or ND1643 there may be a requirement to consider external audit – which is quite clearly a highly unattractive prospect for any CP, and indeed essentially a punitive measure. This text citing ISO27000 was a distinct single addition made by Ofcom in February 2012, which brings it into even sharper focus and arguably gives it greater weight in terms of the perception of Ofcom's expectations.

17. Then in the CFI Ofcom reiterates that its thinking up to this point on section 105A has been centred on ISO27000:

> ***Summary of current guidance***
>
> *4.3* ***Risk management*** *– as a minimum, periodic consideration of main security risks to networks and services and implementation of a plan for appropriate mitigation.*
>
> *4.4* ***Basic security practices*** *– compliance with a general information security standards* ***<u>such as ISO270xx</u>****, and/or other evidence that good practice is followed [..] [emphasis added]*

18. The natural conclusion to draw from the original guidance, and the February 2012 addition, was that ISO27000 (in conjunction with ND1643) would carry significant weight in terms of satisfying Ofcom in this area of the requirements.

19. However, it now appears that Ofcom's focus and emphasis has internally shifted in this area. It suggests in paragraph 4.8 that the ISO27000 standard does not properly align with the objectives of section 105A. It further suggests that other initiatives such as those being developed by the Department for Business Innovation and Skills and/or ENISA will get closer to providing a documented standard which can be used as a starting point for considering compliance with section 105A. It asserts that a version 2 of the ENISA Technical Guideline on Security Measures (the "v2 document"), which it has been collaborating on, will more closely meet its expectations in terms of compliance with section 105A.

[2] Footnote 10

20. Setting aside for a moment the merits or otherwise of the policy change, it is disappointing and concerning that Ofcom considers it acceptable to signal one message to industry about compliance, and then effectively change its mind and expect stakeholders to simply follow a new path regardless of the steps they may already have taken. This appears to be more than simply Ofcom setting out its evolving thinking or complementing its original guidance. It is a fundamental change in the way Ofcom will approach compliance assessment and the external reference to be used as a starting point. This undermines regulatory certainty and will inevitably result in increased costs for CPs. It makes it more difficult for stakeholders to plan and prepare compliance strategy and reduces confidence in any decisions made.

21. Ofcom's policy shift is made all the more difficult to comprehend by the fact that the current ENISA guidance has been around in one form or another since 2011 – yet it is only now that Ofcom decides that ENISA's work in this area should be the focus for compliance with section 105A. Ofcom cites its view that ENISA's guidance offers the "benefits of a common approach" as well as "reflecting good security practice generally" – these are not new concepts so why wait until now to reference this in its policy? At the very least this view could and should have been signalled when Ofcom issued its revised guidance in February 2012. Whether or not Ofcom ultimately adopts its proposed changes, it should recognise the problems and uncertainty it will generate if it feels able to switch from one existing starting point to another – especially as industry has not even seen the latest version of the proposed new ENISA document.

22. In terms of expanding the scope to include supply chains, Ofcom should be aware that it runs the risk of developing significant new burdens both for CPs and itself it is wishes to be consulted on all changes to supply chain arrangements in advance of any material changes. Large multinational CPs change supply arrangements regularly and it would become a very unwelcome burden if we were expected to consult on every such occasion. Again Ofcom needs to see the wider picture, and be prepared to place a degree of trust in CPs. While Ofcom may wish to set out its views on best practice, going beyond that risks a highly unnecessary blanket regulatory burden which will achieve little in the vast majority of cases. Expecting responsible sophisticated CPs, with a deep knowledge and understanding of the relevant security risks and mitigations, to consult on revisions to supply chain arrangements is quite clearly a step too far.

23. In terms of ENISA's guidance, it is as yet impossible to give a fully informed view as the v2 document which Ofcom references is not in the public domain. This is why we consider that Ofcom should pause in its proposals until we see this document. However, as indicated above it is imperative that Ofcom explains in any subsequent consultation the extent to which other EU NRAs are actively considering this guidance as a baseline

NON-CONFIDENTIAL

for Article 13a compliance. The “benefits of a harmonised approach across EU Member States”, which Ofcom describes at paragraph 4.15, will only be realised if this guidance is adopted by the EU community as a whole. Ofcom explains that it has been involved in developing the v2 document, so it should be in a position to do this. Indeed it would have been helpful if it had explained the position of other EU Member States in the CFI, in order to properly assess whether the v2 document really will deliver the harmonisation benefit.

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

24. In relation to this aspect of the CFI, Ofcom will need to focus its attention on those CPs that maintain direct contractual relationships with consumers. While it is important that all CPs adhere to the relevant security obligations, it will be primarily the responsibility of consumer-facing CPs to ensure that they have the necessary SLAs in place with any upstream provider to maintain service availability and to ensure that they are providing transparent information to their customers.

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

25. We agree with Ofcom that in relation to protecting network interconnections (pursuant to section 105A(3)), it is reasonable to advocate ND1643 certification as a means of demonstrating compliance. We consider that in its current form, it is a proportionate measure in that it is relatively inexpensive, appropriately targeted and also flexible enough to work across most if not all CPs regardless of their set-up. The scope also appears clear and well-defined.

26. As expressed in the response to question 3 above, we would expect the provision of consumer related information to be a matter only for consumer-facing CPs, and Ofcom should make this distinction clear in any further consultation and/or revised guidance.

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?

NON-CONFIDENTIAL

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?

27. [✂].

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

28. [✂]. Ofcom should bear in mind at all times that the reporting burden is one which runs alongside the work to actually resolve the incident in question. Therefore the more time that has to be spent in preparing and submitting a report, the more of an impact it will have on the incident. Where CPs have an efficient, well-established and timely reporting process, which provides Ofcom with all the information it needs, it should be allowed to continue with this without further interference. As Ofcom rightly points out at paragraph 5.42, a CP’s focus should be on management and resolution, and reporting requirements should be as light as possible.

Verizon Enterprise Solutions

February 2014