UPDATING OFCOM’S GUIDANCE ON NETWORK SECURITY

SKY RESPONSE

This submission constitutes the response of British Sky Broadcasting Limited (“Sky”) to Ofcom’s call for inputs: ‘Updating Ofcom’s guidance on network security’ (“the NSCFI”), dated 13 December 2013.

Sky recognises the fact that Ofcom’s S105B reporting obligations and related guidance have been in place for two years and may benefit from refinement. However, Sky considers that the process is working well and that the guidance therefore should not be amended to such an extent that it results in more onerous obligations being placed on communication providers (“CPs”). Sky considers it important to maintain a proportionate and flexible approach to incident reporting and to allow CPs to determine their own security policies in accordance with current regulatory requirements.

The remainder of this response will address each of Ofcom’s questions from the NSCFI in turn.

1. 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?

1.1 Although the Detica Report (the “Report”) identifies a number of emerging and evolving risks, it only considers a subset of these risks (non-deliberate) and this is arguably not a sufficient basis for any revised guidance. Sky considers that in order for any revised guidance to be of use to CPs all threats need to be addressed i.e. deliberate and non-deliberate threats.

1.2 We note that the Report does not touch on CPs growing dependency on power and the broader industry wide issues surrounding whether CPs will have enough power to run their networks in the future. Although this is considered a traditional issue, it is one where the specific risks are changing and one that could benefit from further consideration in any revised guidance.

1.3 In any event, Sky constantly reviews its network to ensure that it has adequate protection in place to meet current (and envisaged) security threats. Sky therefore does not consider that further guidance is required to address the risks identified in the Report at this time.

2. 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?

2.1 Sky considers that ND1643 is working well in practice and that, although the ENISA Guidelines (the “Guidelines”) build on this, there is currently no need to go above and beyond ND1643. ND1643 ensures that CPs meet their security and network resilience responsibilities and it can be objectively certified against by an independent third-party. Sky is concerned that any additional requirements would place further unnecessary burdens on CPs.

2.2 However, should Ofcom consider it is necessary to introduce further controls which go beyond ND1643, in Sky’s view, it would be more appropriate for Ofcom to either:

(a) work with the industry and NICC to develop a set of minimum standards; or

(b) to recommend that CPs comply with a certain subset of the 114 controls set out in ISO27001 (as these requirements are well understood).

2.3 As mentioned above, any new obligations to manage general security risks that are introduced as part of a network security guidance update should not place additional disproportionate burdens on CPs.

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

3.1 Sky places great emphasis on maintaining excellent security practices[1], ensuring that customers are aware of the level of security offered and are informed when network issues occur. Sky considers that the processes that it has in place in this regard are proportionate.

3.2 Sky provides information to its customers on network issues that may affect their service in a number of ways: via messaging on sky.com; using recorded messages when customers call into our contact centres; and increasingly using social media. In some circumstances, we also send proactive messages to customers via SMS, email or white mail. Customers can also view information on Sky's network resilience and security on its website[2].

3.3 Currently, CPs have an appropriate level of flexibility when it comes to communicating network issues and security policy to their customers, and Sky considers that there is no need for further involvement by Ofcom.

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

4.1 Sky would welcome additional insight into network availability be way of a root cause based analysis (rather than an analysis based on CP performance). In this regard, we note that Ofcom could build on the Resilience chapter in its 2013 Infrastructure Report (section 6)[3], which included a number of new root causes compared to previous years.

5. 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?

5.1 Sky considers that 'over the top' arrangements are sufficiently monitored and that there is no need for Ofcom to clarify its expectations or extend the scope at this stage.

6. Question 6 - what are your views on the appropriate thresholds for reporting incidents affecting consumers of smaller CPs, mobile networks, data services and services suffering partial failures?

6.1 Sky considers that Ofcom's guidance strikes the correct balance between quantitative and qualitative reporting criteria for larger CPs. The absolute thresholds are sufficient for larger CPs and should be maintained at the current level.

6.2 However, Sky supports Ofcom's view that a mixture of relative and absolute thresholds could be introduced. It is appropriate for Ofcom to consider smaller CPs and not just to

[1] Sky was recently recertified in relation to ND1643.

[2] http://help.sky.com/security/privacy/skys-network-resilience-and-security

[3] http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/infrastructure-report/IRU_2013.pdf

focus on the larger ones, to avoid situations where incidents which are 'significant' to customers of smaller CPs go unreported. Sky considers that it would be sensible to introduce a number of relative thresholds for smaller CPs (linked to a percentage of customers affected) so that information on their incidents is also captured.

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

7.1 Sky is of the opinion that the current process for reporting significant incidents is proportionate, provides sufficient flexibility and is working well. Sky does not consider that there is any need to make changes to this process at the present time.

Sky **21 February 2014**