Response of Sky UK Limited ("Sky") to Ofcom's Review of Security Guidance Consultation

Executive Summary

1. Sky understands and accepts that cyber security issues are of significant importance to the UK economy and supports the aim of managing cyber security risks in line with the increasing threat they pose. However, Sky seeks to manage such risks in a proportionate and effective way, minimising the burden to CPs' businesses.

Section 2: Security and Availability (s105A)

2. Sky appreciates Ofcom's role in ensuring that cyber-attacks do not cause service outages, though Sky notes that the Information Commissioner's Office ("ICO") is responsible for ensuring that businesses appropriate cyber security measures in place to protect personal data. Each organisation's responsibilities should be clearly delineated to ensure clarity and certainty for business.

Paragraphs 2.15-2.16 – Risk management and governance

3. As opposed to an approach based on certification, Sky favours an approach based on identifying specific threats faced, designing and implementing appropriate tests that establish whether attacks can be detected, and assessing the efficacy of the steps taken to mitigate those threats. Such an approach involves continuous learning and improvement and will be beneficial in defending and reacting to more sophisticated cyber-attacks from well-resourced threat actors.

4. While a certification-based approach has the benefit of increased certainty for business, the resulting lack of certainty in a risk-based approach could be remedied by Ofcom providing clear guidance, or engaging with CPs on a case-by-case basis.

5. Sky does not consider it appropriate to proceed with the Cyber Essentials Plus Certification as the costs of such certification would be excessive in relation to the benefits achieved.[1]

6. Sky does however recognise the value of the "TBEST" initiative, currently being led by DCMS, and will consider the adoption of this scheme when it is formally launched.

Paragraphs 2.29-2.31 – Maintaining network availability - Single points of failure

7. Paragraph 2.30 of the Consultation states: "*it is more likely to be disproportionate to deploy protection paths in the access network than in a CP's backhaul and core networks*". This

---

[1] *See* [✂]

seems to inadvertently imply that resilience in the backhaul and resilience in the core networks are equally proportionate steps to take to avoid single points of failure.

8. Sky works diligently to ensure that it has resilience in its core network. However, it is not proportionate to build the same level of resilience in the backhaul as the costs are much greater than the resulting benefits.

9. To increase resilience in the backhaul would require a physically separate path for the connections between the BT Exchanges, where Sky hosts equipment nearest customers, and the Sky PoP sites that host Sky core network equipment. The costs associated with such circuits are considerable. Sky Talk and Sky Broadband services are available in excess of 99.95% of the time and although availability of these services would increase with greater resilience of the backhaul circuits, the cost would be disproportionate to the marginal gain.

10. Sky has complied with its reporting obligations under s105B since their implementation in May 2011. Sky has described to Ofcom the steps it has taken to provide customers with access to emergency services when the backhaul circuit fails. This level of resilience has previously been considered reasonable by Ofcom.

Section 3: Incident Reporting (s105B)

Paragraphs 3.7 – 3.27 – Mobile incident reporting

11. Sky interprets the mobile incident reporting criteria as applying to MNOs. Since the thresholds are based on the impact to network infrastructure, MNOs are better placed to meaningfully report.

Paragraphs 3.28 - 3.35 - Cyber incident reporting

12. Sky is subject to attempted cyber-attacks every day, but to date, they have no customer-service impact. Sky believes it would be disproportionate to report on cyber incidents that do not impact customers. Accordingly, Sky considers it is appropriate to notify Ofcom only of cyber incidents that result in a service loss in accordance with the thresholds set by Ofcom under s105B.

13. It is not appropriate for Ofcom to get involved in so called- "major breaches of data confidentiality", which are regulated by the ICO.

Paragraphs 3.36 – 3.47 – 24/7 reporting process for urgent incidents and subsequent changes to other reporting timescales

14. To provide certainty, Sky would require absolute clarity on the definition of an "urgent incident". Accordingly, only clear, quantitative thresholds would be appropriate.

15. Reporting such an "urgent incident" within three hours of becoming aware of the incident will not always be practical, particularly in the evenings, at weekends or during Bank holidays. Sky supports transparency and would endeavour to provide Ofcom an initial report as soon as practicable. Sky cannot, however, at this early stage, confirm the feasibility of updating its processes to consistently meet an obligation to report within three hours.

16. Sky fears that such short reporting deadlines could impact Sky's incident management process by detracting resources away from responding to and rectifying incidents.

Section 4: Audit (s105C)

Paragraphs 4.3 – 4.11 – Increased use of auditing power under s105C

17. The current guidance provides that a CP may be audited as a "backstop measure in exceptional cases". There is no reason to change this approach – it is proportionate to engage informally as an initial step.

18. Ofcom's current information gathering powers are sufficient to ensure compliance with s 105A and 105B of the Act. The direct costs of an audit and the indirect burden on internal resources are significant and are disproportionate. Information requests are less burdensome and Ofcom can use information requests to request specific information, receiving responses that focus on certain identified issues of interest.

19. Auditing powers should only be used by Ofcom when required to address a significant and real concern.

Sky   **7 September 2017**