Vodafone Response to Ofcom Consultation:

General policy on ensuring compliance with security duties

Consultation on Ofcom's draft general statement of policy under section 105Y of the Communications Act 2003 (Ofcom's "procedural guidance") and

Consultation on Ofcom's draft guidance on resilience requirements in sections 105A to D of the Communications Act 2003 (Ofcom's "resilience guidance")

1. Introduction

Vodafone welcomes the opportunity to comment on the compliance regime associated with Ofcom's revised security powers under the Communications Act 2003. We are fully supportive of the aims of the Act and associated regulation and Code of Practice. In our response to the recent DCMS consultation, attached as Appendix A to this response, we set out that we are either compliant, or have a compliance path to the majority of controls set out in the regulation and Code of Practice. On the remainder, we agree with the aims, but our response proposed changes to the wording to make them achievable, reflecting the skilled resource constraints that the UK industry faces, and absence of industry technical standards for some aspects (e.g. signalling reconstruction).

We are aligned with Ofcom in believing that compliance with each control in the Code is not an event, but instead a journey. We consider that Ofcom's emphasis should be on ensuring that regulated providers have a firm plan to achieving compliance, which is built around the degree of risk of the threat that gave rise to the control, for that specific provider. As such, Ofcom will need to work with individual providers as the risk profile associated with each control will be to some degree unique to the specifics of the networks and services of each provider.

2. Answers to Ofcom questions

1. Do you have any comments on our proposed approach to compliance monitoring?

Principles behind Ofcom's approach to compliance monitoring

We agree with the overall principles behind Ofcom's approach to compliance monitoring. As Ofcom sets out in paragraph 3.7 of the consultation, in the first few years of the regime, its focus must be on ensuring that regulated providers are implementing an appropriate culture of providing secure networks and services, backed up by relevant processes and programmes to implement the technical measures in the Code of Practice.

Although Vodafone has been at the forefront of working with DCMS and NCSC to establish the content of the regulations and Code, we acknowledge that both Ofcom and providers such as ourselves will be on a learning curve in establishing a workable compliance monitoring regime. We will of course work with Ofcom to implement a risk-based approach to improving the security of UK networks.

At a high level, we agree with the approach set out by Ofcom in the consultation. Nevertheless, we must acknowledge that it is only when the detail of the regime becomes clear, for example when there is greater visibility of the format and content of Information Requests, that we will be able to say with confidence that

we're totally aligned with Ofcom. However, we believe that Ofcom is taking the correct track at the outset, and we will work together to ensure that the exercise is a collaborative one.

Ofcom approach to monitoring Tier 1 and Tier 2 providers

It has always been a fact of regulatory life that in the interests of administrative priorities, there has been greater Ofcom scrutiny on large providers such as Vodafone. However, we believe that the regulations associated with the new security provisions of the Act are novel in enshrining a differential compliance regime into law. We are far from comfortable with this approach, and whilst being a matter for DCMS, we consider that Ofcom should have concerns about the impact on its statutory duty to promote competition between communications providers. The regime will not only mean differing compliance costs according to the tier assigned to a given provider, but will also mean that for those provisions of the Code of Practice that have different compliance dates according to tiers, providers will face differential regulation over the next few years. To the best of our knowledge, such differential regulation has only ever previously been the case where a provider has objectively been established to have significant market power, and the different compliance costs will inevitably distort competition to some degree.

It could be argued that it is more important that Tier 1 providers comply with the Code early because the ramifications of a breach are greater for such providers than those in Tier 2/3. However, this is a flawed assumption – for example ✂. It is simply wrong to consider that important services and critical national infrastructure are solely the purview of Tier 1 providers – indeed given the cost of early compliance with the Code, the ripple-through to retail pricing could nudge the relevant customers into making more purchases in the Tier 2/3 space.

The differential timing also impacts on competition within the Tier 2 community. Tier 1 providers typically outsource some functions to Tier 2 providers, for example to access network providers. In order to comply with the regulation, this means that Tier 1 providers will need to bootstrap the Tier 2 subcontractors to meet the Tier 1 deadlines via contractual provision:

- Firstly, this puts the Tier 1 provider in the uncomfortable position of being a pseudo-regulator to ensure that the Tier 2 provider meets the Code; we urge Ofcom to take a proportionate approach to compliance in this area, i.e. that it is sufficient that the Tier 1 provider makes reasonable efforts to ensure compliance in this situation, for example by contractual provision, rather than any expectation that the Tier 1 provider will establish a "shadow Ofcom security team" to audit the Tier 2's compliance.
- Secondly, it is impossible for this contractual back-ending to fully incorporate pass-through of liability. The maximum penalty faced by a Tier 1 provider for non-compliance will typically be larger than the overall turnover of the Tier 2 provider, making it impossible for them to take on this risk. Again, we urge Ofcom to take a proportionate approach where issues arise in this situation.
- Finally and importantly, if some Tier 2 providers are forced by contract to adhere to the Tier 1 timelines, but others don't have such wholesale arrangements and can thus adopt the Tier 2

timelines, this inevitably affects competition more widely between Tier 2 providers. This could mean competitive distortion, or could mean that Tier 2 providers decline to subcontract to Tier 1 providers because of the increased cost burden; either outcome should concern Ofcom.

For these reasons, we believe that the only reasonable outcome is if the compliance deadlines are aligned for Tier 1 and Tier 2 providers (with these deadlines being those that are currently proposed for Tier 2 providers).

Notwithstanding these points, if the tiering concept remains, we are comfortable with the procedural approach adopted by Ofcom. Although the concept of relevant turnover being a proxy for relative importance of a provider is flawed, we believe that it is the most readily and objectively applied metric. We see no reason to "re-invent the wheel" in coming up with a scheme that determines the tier to which a given provider is assigned. Given Ofcom already holds this information, we're somewhat surprised that para 3.14 of the consultation suggests that the exercise could take more than three months, as each provider should already know which tier it falls into – all that should be needed is a letter from Ofcom formalising this information (in the alternative that there is some doubt as to the relevant turnover of a given organisation, we would have expected Ofcom to have already been pursuing the matter under the activity of payment of the correct Network & Services fee).

Information-gathering powers (section 135)

Usage of S.135 Information Requests is the approach that we would have expected Ofcom to adopt, so we are supportive. This said, it is impossible for us to give unequivocal confirmation that we are comfortable, until such a time that we see the format of the S.135 requests.

Superficially, with 253 controls in the Code (60 of which have more than one target compliance date associated), generating S.135 requests on a six-month cycle may mean that each request will contain an enormous breadth of information. It may therefore be better to adopt an approach of more frequent smaller S.135 requests, reflecting that providers could be compiling the response to one S.135 whilst Ofcom processes the content of the previous one (NB it would still be essential that each S.135 went through the process of being shared in draft form for comment before being finally issued).

Given the volume of controls hitting their compliance dates ebbs and flows over coming years, Ofcom may also need to consider whether it has the necessary bandwidth to examine compliance with a given control at the time set out in the Code. Much as providers will be adopting a risk-based approach to achieving compliance, Ofcom will similarly need to prioritise its finite resources to adopt a risk-based approach to assessing compliance.

We note that Ofcom's proposes to allow Tier 2 providers longer to respond to S.135 requests than Tier 1. This is counter-intuitive, as Tier 1 providers will inherently have far more complex and parallel systems, being larger organisations with (on the whole) a wider set of services provided. We therefore believe that the response times for S.135 requests should be the same, regardless of organisational size.

The wealth of information provided by industry in response to S.135 requests will be incredibly sensitive. Ofcom must acknowledge that it will itself become a security risk, being a central repository of the security strengths and weaknesses of UK providers. All avenues must be explored to minimise this risk. ✂ Additionally, we will need assurances around data retention, disposal, and access policies before we can share sensitive information.

Power to direct providers to explain any failure to act in accordance with a code of practice (section 105I)

We accept Ofcom's approach, but note that the Code of Practice states that the Code is not the only way to meet security duties and providers may choose to meet these in other ways. Ofcom will therefore need to work collaboratively with providers to agree whether alternative measures and technical solutions are appropriate.

Powers to assess compliance – Assessments and assessment notices (sections 105N-105Q)

We are comfortable with the approach.

Powers to assess compliance – Power to enter premises (section 105O and 105R)

We accept Ofcom's powers, but would hope that this will never be necessary in our case.

2. Do you have any comments on our proposed approach to testing?

Vodafone notes Ofcom's comments on testing under s105O. As Ofcom will be aware, ✂

3. Do you have any comments on our proposed approach to enforcement?

Everyone should share the goal of improving the security of UK networks, that motivates implementing the changes to the Communications Act in a timely manner. We hope that our relationship with Ofcom will be a collaborative one on a shared journey to compliance.

There is a fundamental tension between Ofcom's ability to take enforcement action, and the desire to ensure that there is pan-industry learning from shortcomings identified in individual providers. We need to foster a culture like the aviation industry, where the identification of issues is seen as an opportunity for learning. However, the danger is that the threat of penalties means providers restrict information to the bare legal minimum.

To avoid a "cover up culture", enforcement action should therefore be an absolute last resort where a regulated provider is wilfully negligent in failing to take action towards compliance with the Code, or remains non-compliant without carrying out a risk assessment, or gives the compliance exercise an inappropriately

low priority. In these circumstances we would support enforcement action on Ofcom's part, otherwise we would have the situation where providers could seek to gain competitive advantage by either prioritising spend on more commercially attractive propositions, or by having a lower cost base by not bothering to dedicate the resources required to have a robust security environment. We believe that the proposed approach to enforcement set out in the consultation provides every opportunity for regulated providers to mend their ways and work collaboratively with Ofcom.

4. Do you have any comments on our proposed approach to reporting security compromises?

Duty under s105J to inform users of risk of security compromise

We welcome Ofcom's clarification at para 5.3 that they would not expect providers to inform end users of potential or actual security compromises where there is unlikely to be an adverse effect on the user.

As a new piece of legislation, we consider that the duty to inform users will take some time to bed in, with collaboration once again required between Ofcom and providers to establish a shared decision tree of when it is appropriate to engage customers, backed up by examples that emerge over time. We consider that the dangers of over-reporting (in terms of loss of confidence and confusing customers with repeated warnings, particularly if there isn't any reasonable action that could be taken by the customer) are as relevant as those of under-reporting. As an industry, we will need to agree a consistent regime that strikes the right balance.

Security compromise reporting to Ofcom under s105K

We believe that significant work is required in this area. The existing s105 guidance incorporated the notification of security incidents, but the operation of it was far from clear. ✂

Whilst the numerical thresholds set out in Annex 1 are suitable for determining whether outages should be reported (subject to our observations below), they are ill-suited to security compromises: the implication is that nothing is reportable unless service is lost or disrupted. This leaves the provider decision of whether to notify largely being oriented around qualitative criteria, but the main threshold of "*major cyber security breaches"* leaves considerable latitude meaning that Ofcom is unlikely to receive reports on a consistent basis from the provider community. Greater clarify of what Ofcom regards as a *"major cyber security breach"* is required.

We believe that the approach set out in para 5.14, i.e. that providers should notify Ofcom of a breach where an attacker could have used an initial breach to mount a further attack and cause significant effects, will result in over-reporting where providers have measures in place to prevent that further attack. It is important that Ofcom focusses on key threats to UK infrastructure, and by placing this requirement we believe that there is a risk of being overwhelmed.

Realistically, it is unlikely that the requirement set out in para 5.21, i.e. that major security compromises be notified to Ofcom within 3 hours, will be consistently achievable. On occasions where there is a major security compromise, our focus must be on the protection of our infrastructure and customers. We will notify Ofcom as soon as is reasonable and in particular where the breach is likely to have ramifications for third parties (e.g. other providers), but it must be understood that in these situations notifying Ofcom is of secondary importance. We therefore cannot commit to a 3-hour SLA, but will make all reasonable endeavours to notify Ofcom as soon as possible.

We note at para 5.36 that Ofcom will provide annual reports to Government under Section 134A and 134AA of the Act. We recognise that this is an obligation on Ofcom, however extreme care must be taken in compiling these reports. The reports must be summarised at a level such that if there was a breach that the report itself was made available to third parties, this would not further compromise the security of UK networks. Further, care must be taken to ensure that any release of information does not disrupt the market, for example by naming and shaming network operators.

In the context of which incidents and outages are reportable, we believe that minor amendments proposed by Ofcom to the numerical thresholds will have consequences that may have not be foreseen. In the previous guidance, there has been a note on the mobile network thresholds that because of the complexity of establishing how many end users are affected, criteria would be agreed bilaterally with mobile providers[1]. This note has been removed, presumably in the interests of seeking consistency of reporting, meaning that the thresholds are entirely set by Table 2 in Annex 1. However, Note 2 to Table 2 exempts reporting where customers could have roamed onto third party networks to retain 999 access. As the UK mobile providers have implemented Limited Service State roaming, this Note 2 will always apply where another mobile network is present, i.e. it applies other than the narrow case of mobile Partial Not Spots (PNS) where the mobile provider with the incident/outage is the sole provider of coverage in that area. Given the metrics in Table 2 are voice-oriented, the PNS situation will rarely apply, as the mobile providers have an existing licence obligation to provide service in >90% of geography, meaning the "narrow case" where Note 2 wouldn't apply would be perhaps 2-3% geography. As such, the only time where reporting would strictly be needed is if 100,000 people were affected by a service outage within the 2-3% of geography where the provider is the sole network with coverage. In effect, the proposed Table 2 means mobile outages need *never* be reported by mobile network operators. Bizarrely, as Note 2 doesn't apply to the MVNO line of Table 2, MVNOs are not captured by this loophole and are still required to report. Vodafone would be comfortable if this matter was resolved by removing Note 2 to Table 2, i.e that reliance on Limited Service State roaming would not exempt providers from the need to notify outages.

[1] For the avoidance of doubt, although Vodafone nominally uses the thresholds set by our major incident management process, we have taken full account of the numerical thresholds in Table 2 and for example notified any outages where >1000 customers lost access to emergency calling for more than 1 hour.

5. Do you have any comments on our proposed approach to information sharing?

We understand the need for information sharing and are broadly comfortable with the measures set out in the consultation. However, given the extreme sensitivity of the information involved, more work is required to develop a comprehensive information management policy. This must include not just what information is released to whom, but also the usage that it will be put to, the security controls in place by the recipient, and measures to determine that the information is securely destroyed when no longer required.

6. Do you have any other comments on our draft statement of general policy set out at Annex A5 to this consultation?

No further comments.

7. Do you have any comments on our proposed approach to resilience set out in section 4 of the draft guidance at Annex A6 to this consultation?

How Ofcom uses its powers

As set out in our response to Question Three, there is a tension between fostering a culture of industry learning from resilience issues, and Ofcom's ultimate ability to take enforcement action. We agree with the approach set out in paras 4.2-4.4, and have a history of working with Ofcom to use resilience events as an opportunity for organisational learning.

Sources of resilience guidance

We note the documents identified by Ofcom; Vodafone has been active in the production of many of these documents and will take account of their contents.

We note the reference at para 4.16 and 5.27 to NICC ND1653, and also that Ofcom has written to network providers encouraging its adoption: at this stage we consider that it would be premature to incorporate ND1653 into the regulatory guidance. At the outset of NICC developing ND1653, Vodafone was clear that we would not support the adoption of a "UK special" standard in this area, and that any standard must be internationally harmonised. We therefore encouraged the authors to take the material to IETF, where regrettably there was limited support. Vodafone did not oppose the publication of ND1653, because it was made clear that it was an optional standard to be used by those network providers who wished to adopt dynamic overload control measures. Having surveyed all of Vodafone operating companies globally, we had not identified any jurisdiction that had taken such an approach so therefore intended to adopt static controls. Had the NICC standard been a mandatory one, we would have objected during the approval process.

✂

We are liaising with our vendors as to the feasibility and implications of adopting ND1653. Until we, and other providers, have had the opportunity to complete this exercise, then it is premature to incorporate it into the resilience guidance.

8. Do you have any comments on our proposed resilience guidance set out in section 5 of the draft guidance at Annex A6 to this consultation?

Noting our position regarding ND1653 in response to Question 7, we note and accept the guidance.

There is a sense, however, that at times we are involved in a game where it is clear that the aim is to score a goal, but where the referee is withholding the finer points of the offside rule until the point at which the linesman raises their flag. Whilst recognising that Ofcom cannot give up-front advice on every matter of resilience, there are topics that would benefit from Ofcom driving common industry positions. For example:

- Resilience of interconnection. We are moving from a TDM world where, for example, Vodafone interconnected to 600+ BT nodes across 70-100 physical handovers, to one where there are a limited number of logical and physical connections of much greater size. The commercial arrangements mean that originating networks neither know nor care about where in the terminating network the call is destined, meaning there is no [commercial] incentive to minimise the number of callservers in the call path. ✂. We believe that there is a need for an industry debate on resilience of networks in case of interconnect failure.
- Resilience of access networks. In working with our access network partners, Vodafone has agreed standards about the degree of network diversity that is proportionate for a handover serving a given volume of customers. However, this is based on our own risk assessment, and this necessarily means that other providers will have taken different views. We believe that there is a need for consistency in this area.
- Power resilience. We have an ongoing conversation with Ofcom in this area, both in respect of resilience of consumer fixed services, but also of the mobile network as fixed providers increasingly encourage customers to rely on their mobile device when there is a power outage. We do not wish to rehash the debate in this response, but note that greater power resilience is not cost-free, and that challenging market conditions mean that we are unable to recover any increased costs commercially. Given that most consumers will be directed to using their mobile devices during a power cut, with the UK mobile networks becoming networks of last resort, there is a clear need to provide a route to fair funding for the provision of public good levels of resilience. We look forward to working with Ofcom, other sector regulators and Government, to advance the conversation.

9. Do you have any other comments on our draft guidance set out at Annex A6 to this consultation?

We draw your attention to our observations of the working of the quantitative reporting thresholds in our response to Question Four.

Vodafone UK

May 2022

Appendix A – Vodafone response to DCMS consultation: “Proposal for new telecoms security regulations and code of practice”

✂