NON-CONFIDENTIAL

General policy on ensuring compliance with security duties

Response to Ofcom's consultation

May 2022

Executive summary

Sky supports the overarching principles of the new security framework established under the Telecommunications (Security) Act 2021. Improving telecoms security is an important step in managing and supporting the UK's role in the global digital economy.

The Telecommunications (Security) Act 2021 and accompanying Regulations and Code of Practice represent a major overhaul of cyber security regulation in the UK. Sky welcomes the collaborative approach which Ofcom proposes to adopt in fulfilling its role of ensuring that telecoms providers take appropriate and proportionate measures towards full compliance. Such an approach is essential as, in monitoring and enforcing compliance with the new framework, Ofcom should not underestimate the technical complexity and scale of the changes that providers will need to implement over the coming years.

Furthermore, Ofcom's collaborative approach to monitoring and enforcement needs to be flexible and proportionate. This should include giving providers a reasonable and proportionate amount of time within which to make the necessary changes, enabling providers to focus on prioritising those changes which address the greatest security risk.

The proposed timescales set out in the draft Code of Practice do not take account of the number, size and nature of the challenges which providers face in complying with the new framework [redacted]. Sky therefore urges Ofcom to begin engaging with providers as soon as possible, to ensure that the timescales and wider approach which Ofcom takes towards monitoring and enforcement are fair, reasonable and proportionate.

Introduction

Sky supports the aims and objectives of the Telecommunications (Security) Act 2021 ("**TSA**"), the draft Electronic Communications (Security Measures) Regulations ("**the draft Regulations**") and the draft Code of Practice ("**the draft Code**"). The new framework will require telecoms providers to implement significant and technically complex changes over the coming years. Sky therefore welcomes Ofcom's intention to engage with industry and to adopt a collaborative approach towards monitoring and enforcing compliance.

Nevertheless, it is essential that, from the outset, the substantial challenges which providers face in implementing the new framework are reflected in Ofcom's anticipated timescales for compliance and early and ongoing engagement with providers.

Timescales for compliance must be reasonable and proportionate

Overall, Sky considers the proposed timescales for compliance to be unreasonable and disproportionate. In the draft Code, there are a total of 253 measures, 125 of which currently have a proposed compliance deadline of 31 March 2023. This would require providers to put into place almost half of the guidance measures within six months of the Regulations coming into effect.

The proposed timescales are neither technically feasible nor practical due to:

- other long-term strategic security-related projects, the most onerous being the Government's direction to providers to remove Huawei equipment and services from the UK's telecoms networks, which must be prioritised due to the pre-existing statutory deadlines. [redacted];
- legacy equipment, which all providers will have installed in their networks, and for which the network or solution would need to be redesigned. [redacted];
- the additional work and time it will take to amend agreements with [redacted] third party suppliers;
- the increased risk of service outages occurring as a result of introducing a significant number of system changes within a short period of time; and
- the delay caused by increased competition, including from Ofcom and DCMS, for skilled workers within a finite pool of expertise. [redacted]

[redacted] the proposed timescales for compliance by Tier 1 Providers, in particular, are impracticable and disproportionate. [redacted]

[redacted]. This demonstrates the need for Ofcom to approach its monitoring and enforcement role in a reasonable and proportionate way that recognises the enormous challenges which providers face.

Importance of early engagement

Ofcom expects to notify providers which tier they fall into under the proposed tiering system within three months of the new framework coming into force. Ofcom suggests that, depending on the information it receives from individual providers, less than three months' notice may be provided.

Given the scale and complexity of the changes that providers need to make, it would be inadequate and unfair to give providers such short notice. Sky urges Ofcom to extend the notice period beyond three months and, in any event, to engage with providers as soon as possible, to ensure that Ofcom has the information it needs to be able to issue tiering notifications in good time.

[redacted] early engagement is required for providers to obtain the following clarifications on scope[redacted]:

- the scope of 'Security Critical Functions' and 'Network Oversight Functions';
- guidance on the application of the Supply Chain requirements in draft Regulation 7 to third party network providers and Transit Network Operators;
- application of the virtualisation measures in the draft Code to public cloud services;
- application of the requirement to redesign existing networks in draft Regulation 3(1)(b) to the growth of existing networks;
- how DCMS/Ofcom intend to deal with situations where third party suppliers to Tier 1 Providers are unable or unwilling to comply with the Tier 1 requirements; and

[redacted]

[redacted]

Timing and scope of information requests

Ofcom suggests that the first section 135 information request will be issued on 1 January 2023, with providers to have four months within which to respond. Sky is concerned that this will be just one month after the deadline for the first phase of compliance, for 123 measures, which is currently targeted for 31 March 2023. This seems impractical for both providers and Ofcom – neither soon enough prior to the proposed 31 March 2023 deadline to allow providers to act on any feedback provided by Ofcom, nor long enough after the deadline to enable providers to comprehensively report on compliance as at the proposed deadline date.

Regardless of whether the proposed compliance deadlines remain in place, it would be more appropriate for Ofcom to engage with providers as soon as possible and to request information on an informal basis, in the first instance. This will help ensure that Ofcom avoids disproportionate and unnecessary section 135 requests, and provide greater certainty, earlier, to the benefit of both Ofcom and providers.

Regulatory burden must be minimised by prioritising higher risks

Telecoms providers will incur substantial costs in working towards full compliance, particularly given the unreasonable and disproportionate proposed timescales (discussed above). Examples of cost drivers which Ofcom could have some influence over include:

- additional skilled and experience workers to implement and operate the guidance measures, the cost of which will be higher if providers are driven to implement the necessary changes using third party consultants (of greater expense than in-house resources). Increased demand for limited resources will further increase costs;
- early replacement of legacy equipment from vendors that also need to satisfy additional guidance measures during the execution of contracts. [redacted];
- support needed to maintain services, to be provided from within the UK. Sky urges Ofcom to adopt a proportionate interpretation of risks related to 'national resilience' measures, in order to address providers' existing operating models; and
- resourcing involved in responding to additional information requests from Ofcom, which Ofcom can minimise by, as much as possible, engaging with providers informally and by only requesting information which Ofcom strictly needs in order to carry out its functions under the new framework.

Sky considers that, in its approach to monitoring and enforcing compliance with the new framework, Ofcom should focus on the most significant risks. Providers should be able to replace equipment affected by lower risk measures according to their planned replacement of legacy equipment, following engagement with Ofcom. [redacted] it is important that the measures are reasonable and proportionate.

Responses to consultation questions

Questions concerning Ofcom's draft general statement of policy under section 105Y of the Communications Act 2003

Q1. Do you have any comments on our proposed approach to compliance monitoring?

Importance of effective collaboration between Ofcom and providers

Sky welcomes the collaborative approach which Ofcom proposes to adopt in fulfilling its role of ensuring that providers take appropriate and proportionate measures towards full compliance. Given the scale and technical complexity of the changes which providers will need to make to their networks, it is important that there is early dialogue and industry engagement, where Ofcom can informally gather information and work with providers to proactively address challenges (with formal enforcement to be used a last resort, only where a provider refuses to adequately engage with Ofcom).

Changes needed to the proposed tiering system

Sky is not opposed to the principle of tiering. However, Sky does object to the assumption which underpins the proposal to use the tiering system to determine other elements of the regime (including earlier dates for compliance by Tier 1 Providers, than Tier 2 and Tier 3 Providers), that the size and scale of Tier 1 Providers means that they can more quickly implement the necessary changes.

Sky considers the proposed dates for compliance by Tier 1 Providers to be unreasonable and disproportionate. The timescales for Tier 1 Providers should instead be pushed back by an additional two years, to align with the timescales for Tier 2 Providers. [redacted]

Need for a flexible and proportionate approach to information gathering

Ofcom envisages a rolling programme of information requests, which it expects to 'broadly align' with the timescales in the draft Code and "*well in advance of these dates wherever possible*". In its clarification published on 20 April 2022, Ofcom states that, "*where timescales allow and it is appropriate to do so*", stakeholders will be given the opportunity to comment on draft section 135 information requests. Sky considers this to be insufficient.

Telecoms providers are already experiencing an increase in information requests from Ofcom more generally. To keep the additional resource burden on both Ofcom and providers, as a result of information requests under the new framework, to a minimum, it is imperative that Ofcom engages with providers well ahead of issuing formal information requests, gives providers the opportunity to comment on draft requests and uses formal information requests only where strictly necessary.

Ofcom's ability to build effective technical relationships with providers' technology teams will be as important as using its formal information gathering powers. It is also an essential part of making the journey towards full compliance collaborative. This will rely on achieving some stability in the Ofcom staff supervising each provider and those staff being available for open discussions on a regular basis.

As noted above, it is also important that Ofcom only requests information, which is necessary for its monitoring activities, given that Ofcom centrally holding a large amount of information about the UK's telecoms networks (much of which will be sensitive), itself poses a security risk. Sky would like to understand what safeguards Ofcom will be putting in place to protect such information from potential threat actors. In any event, as noted in response to Question 5 below, Sky proposes that a more appropriate approach would be for information to be stored by each provider in systems which they control, with access given to named individuals within Ofcom, DCMS and NCSC.

Clarifications required from Ofcom

In order to assess the appropriateness of measures taken by providers, Ofcom will need to understand a provider's full range of Security Critical Functions ("SCF"), as defined in the draft Regulations, and which are Network Oversight Functions ("NOF") for the purpose of the draft Code. Ofcom states that developing this understanding will form an "*important objective*" of its early information requests. It is therefore important that there is clarity on all sides as to the meaning of SCF and NOF.

However, the current definitions of SCF and NOF are subject to broad interpretation, and providers have not yet been given the opportunity to raise this with DCMS, Ofcom or NCSC. [redacted], Sky would like to understand what is meant by SCF and NOF.

The definition of NOF in the draft Code suggests that any Operational Support Systems ("OSS") will be within scope. However, the criteria and process for defining OSS has not yet been communicated to providers. Sky proposes the need for a distinction to be drawn between network OSS and subscriber management OSS, and confirmation that subscriber management OSS are out of scope. Clarity is needed for providers and Ofcom to assess this. Sky suggests that the creation of a specific industry forum for discussing such topics would help develop the necessary clarity.

As noted above, [redacted] Sky also seeks clarification in relation to:

- application of the Supply Chain requirements in draft Regulation 7 to third party network providers and Transit Network Operators;
- application of the virtualisation measures in the draft Code to public cloud services;
- application of the requirement to redesign existing networks in draft Regulation 3(1)(b) to the growth of existing networks;
- how DCMS/Ofcom intend to deal with situations where third party suppliers to Tier 1 Providers are unable or unwilling to comply with the Tier 1 requirements; and

[redacted]

Q2. Do you have any comments on our proposed approach to testing?

[redacted] Sky supports Ofcom's proposal to continue to run TBEST as a voluntary, open and collaborative program. [redacted]

[redacted]

Q3. Do you have any comments on our proposed approach to enforcement?

Ofcom's enforcement action should be evidence-based, proportionate, consistent, accountable, transparent and targeted, as is required by its general duties under the Communications Act 2003 (as amended by the TSA). It would, however, be useful to providers if Ofcom could clarify the criteria which it intends to apply in deciding when to initiate formal enforcement action, given that (as part of this consultation process) providers have already flagged the challenges which they will face in working towards full compliance.

Sky welcomes Ofcom's intention to adopt a proactive approach to managing security risks. However, given the significant amount of information that providers will be sharing with Ofcom about their systems and processes (much of which will be sensitive in nature), it would be unfair and inappropriate if Ofcom was to use this information to take formal enforcement action without first giving providers the opportunity to address any compliance concerns. Sky therefore strongly urges Ofcom to work in close collaboration with providers, to minimise the risk of unnecessary and counterproductive formal enforcement action, for the benefit of both providers and Ofcom.

Q4. Do you have any comments on our proposed approach to reporting security compromises?

Reporting obligation to users

Sky considers that the proposed obligation on providers to report to individual users on the risk of security compromises occurring would be unreasonable, counterproductive and unnecessary.

Firstly, an obligation to publicise network vulnerabilities could have adverse consequences. It could be seen as an invitation to potential threat actors to take advantage of such vulnerabilities, particularly if providers are required to directly notify users on an individual basis. Ofcom has not indicated whether it has considered what safeguards would be needed in order to mitigate this risk.

It would also be unrealistic and disproportionate to expect providers to report to users on any and all risks of security compromises occurring. Ofcom needs to clarify the circumstances in which the threshold for providers to report to users would be met, noting that such circumstances should be reasonable i.e. limited to incidents which impact on service and/or security KPIs (such as network-wide service availability) and proportionate, including to the risk faced by users.

Furthermore, Ofcom has not addressed how it would expect users to benefit from this obligation. It is unclear what tangible benefit users would gain from being provided with information on the risk of a security compromise occurring which does not, in practice, impact on the service which they received. Users are protected by the Auto Comp scheme, which was created to manage customer expectations and compensate them for service interruptions. Informing users about the risk of a security compromise is likely to lead to confusion and raise unnecessary concerns, especially if individual users are contacted directly. It is also unrealistic to expect providers to individually report to users on the risk of security compromises occurring. The larger the provider, the more logistically difficult this would be. Also, to justify this, the potential benefits would need to be clear and Sky does not consider this to be the case (quite the contrary).

A more reasonable and appropriate approach would therefore be for Ofcom to limit this obligation to providing users with information on incidents which actually impact on service and/or security KPIs, and via indirect communication channels (e.g. on the provider's website).

Obligation to report to Ofcom

Sky considers the possible scope and timing of this obligation to be unreasonable.

The obligation for reporting "security compromises" that are cyber in nature (e g. a pre-positioning attack), but have ***not*** caused a "resilience" incident is fundamentally new in nature [redacted]. Also, the range of cyber security compromises covered by this obligation is potentially very broad and requires further definition by Ofcom. For instance, it appears that something like the compromise of a single administrator's security credentials (e.g. through phishing) could be reportable to Ofcom and, without further guidance, the reporting volumes would therefore be significant, onerous and disproportionate. Ofcom should not underestimate how significant an undertaking it will be for providers to implement new processes to gather and validate information for the purpose of fulfilling this obligation.

In the clarifications published by Ofcom on 20 April 2022, Ofcom states:

> *"The new framework, including this new reporting obligation (s.105K), comes into force from the commencement date, which is expected to be 1 October 2022. Providers will need to ensure they are ready to report any relevant incidents from this date, in order to meet their legal obligations."*

This proposed timing is unrealistic and disproportionate. Even if DCMS and Ofcom were to publish the outcomes of their respective consultations and provide the necessary clarifications in June 2022 (which is unlikely), it would give providers only three months over the summer from publication of the final Regulations and Code to establish the necessary reporting processes. Also, as noted above, the precise scope of the obligation has yet to be confirmed by Ofcom. Providers need to know the precise scope of the obligation in order to put the necessary processes in place. Sky suggests aligning the compliance date for this obligation with ***at least*** the first proposed compliance date for the obligations contained in the draft Code.

Industry will require further guidance from Ofcom on what should be reported as the current guidance could be interpreted very broadly and impose a disproportionate regulatory burden on providers.

In addition, Sky would echo techUK's calls for Ofcom to try to minimise the likelihood of double reporting by coordinating on security risk reporting by providers with other regulators (subject to Sky's comments on information sharing in response to Question 5 below).

Q5. Do you have any comments on our proposed approach to information sharing?

Sky considers that Ofcom needs to be more transparent and precise about its proposed approach to information sharing. This is important given the nature and volume of information that providers will be conveying to Ofcom.

Firstly, Sky understands the need for certain information sharing to enable Ofcom, DCMS and NCSC to perform their respective functions, including supporting policy development, helping identify new threats and vulnerabilities, and ensuring that the new framework keeps up with evolving threats and technologies. However, Sky and other providers will be expected to share a significant amount of commercially sensitive and confidential technical information with Ofcom, which would represent a material security risk in itself if centrally held by Ofcom. As an alternative, it would be more appropriate for the information to be stored by each provider in systems which they control, with access being controlled by the provider to named individuals within DCMS, Ofcom and NCSC. [redacted].

Secondly, Ofcom says that it may also share information with "*other bodies on an ad hoc basis*", citing the ICO as an example. Ofcom goes on to say that it expects to notify providers about what information will be shared with other bodies and "*where appropriate*" seek consent from providers, unless "*specific circumstances*" justify a different course of action. Sky seeks assurance that Ofcom will not disclose any information which it obtains from Sky without Sky's consent (in accordance with section 393(1) of the Communications Act 2003), subject to the limited exceptions to this set out in section 393(2) of the Communications Act 2003. If Ofcom is proposing to depart from this legal framework, then it needs to be transparent and clarify the 'specific circumstances' in which it envisages that it would be justified in doing so.

Sky would also echo techUK's concerns about the security risk posed by Ofcom centrally holding a large amount of sensitive information relating to the security of the UK's telecoms networks. As noted above, Sky considers that a more appropriate alternative approach would be for information to be stored by each provider in systems which they control, with access being controlled by the provider to named individuals within DCMS, Ofcom and NCSC.

As an overarching principle, it is important that Ofcom's policies encourage open and collaborative discussion with industry bodies and individual providers.

Q6. Do you have any other comments on our draft statement of general policy set out at Annex A5 to this consultation?

No further comments.

Questions concerning Ofcom's draft guidance on resilience requirements in sections 105A to D of the Communications Act 2003

Q7. 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?

In carrying out its functions in relation to resilience, it is important that Ofcom recognises the fact that providers have typically undertaken resilience risk assessments as part of the engineering design process. It will, therefore, take time for providers to implement the new risk assessment procedures required by the Regulations and Code once published in final form. If Ofcom's intention is to use the risk reporting obligations under the TSA to inform future guidance on resilience, it needs to allow providers appropriate time to achieve mature risk reporting across all existing networks. Information requests issued for this purpose should, therefore, be sufficiently targeted at areas of highest priority, so that providers can focus their resilience risk assessment and management activities in those areas.

In section 4 of the draft guidance at Annex A6 to the consultation, Ofcom states that in carrying out its functions in relation to resilience, it will consider its Enforcement Guidelines for regulatory investigations and certain other sources of resilience guidance. However, Ofcom's expectations of providers as regards such additional sources of resilience guidance is currently unclear. Ofcom will expect providers to "*consider*" such sources to the extent that they are relevant to their operations (paragraph 4.12) and, when assessing compliance in relation to a particular resilience matter, "*will seek evidence that a provider has taken account of industry standard resilience best practices*" (paragraph 4.11). Yet as Ofcom notes, these additional sources of guidance do not form part of Ofcom's guidance. Therefore, if Ofcom is expecting to effectively 'enforce' the additional sources of guidance, then it needs to clarify more specifically what it is that it will expect providers to do.

Q8. 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?

To minimise the risk of future compliance concerns, Ofcom "*strongly encourages*" providers to discuss with it, at an early stage, any planned new arrangements that may have significant resilience implications (paragraph 5.17). However, Ofcom does not expand on how this engagement process will operate. In order for providers to understand the potential impact of such engagement on their procurement processes and timescales, it would be helpful if Ofcom could clarify:

- the criteria for supplier engagements to be considered resilience risks about which providers should seek early engagement with Ofcom;
- at what stage of the procurement cycle a provider should seek engagement; and
- the timeframe for a response be provided following any engagement.

Paragraphs 5.22 and 5.30 require providers to consider the risk to end-users as part of any resilience assessment. Sky interprets the reporting thresholds (updated by Annex A5 to the consultation) as Ofcom's guidance on acceptable end-user impact levels. Sky notes that these thresholds have not been changed as part of this consultation.

As identified in response to Question 4 above, there is a lack of clarity as to Ofcom's expectations around the proposed obligation on providers to report to end-users on the risk of security compromises occurring (which is referred to at paragraph 5.23 of Annex A6). Further guidance on appropriate reporting to both consumer and business markets would help providers to publish suitable information. Sky suggests that for the consumer / SME market, it would be appropriate for providers to report annual core network availability, together with service restoration objectives for last mile faults, via the Sky website. However, further industry alignment on the technical definition of any metrics would be required to make such claims comparable between different providers.

Q9. Do you have any other comments on our draft guidance set out at Annex A6 to this consultation?

Reporting obligation to users

For the reasons noted in response to Question 4 above, Sky considers that the proposed obligation on providers to report to individual users on the risk of security compromises occurring would be unreasonable, counterproductive and unnecessary. This would particularly be the case if providers were required to report Resilience Incidents to users. Ofcom states that the occurrence of a Resilience Incident that has had a significant effect on the operation of a network or service will need to be reported to it as a security compromise (paragraph 5.35 of Annex A6). Ofcom should clarify that the obligation on providers to report to users on the risk of security compromises occurring is limited to incidents which actually impact on service and/or security KPIs, and via indirect communication channels (e.g. a provider's website).

Responsibility for third party non-compliance

Ofcom expects providers to have sufficient levels of effective control over third parties and continuous and rigorous checks in place to ensure that actions undertaken by third parties, on behalf of providers, do not put the provider in breach of their obligations under the resilience requirements (paragraph 5.53 of Annex A6). It is unreasonable to expect providers to assume responsibility for non-compliance by third party suppliers, beyond ensuring that contractual arrangements incorporate the resilience requirements. Ensuring such contractual protections is likely to be a significant undertaking for providers, and one that will take a significant amount of time due to the need to undertake the necessary risk assessments first before entering into contractual negotiations. In addition to recognising the amount of time that it will take for providers to amend their contracts, Ofcom therefore needs to clarify its intended approach to non-compliance by third party suppliers. Any such approach must be both reasonable and proportionate.

Ofcom's collaborative and proportionate approach should also apply to resilience

The proposed obligations imposed on providers by the resilience requirements are likely to be onerous. As noted above, Ofcom should not underestimate the extent of the changes which providers will need to make and the time that this will take. Accordingly, it will be important for Ofcom to adopt a similarly collaborative and proportionate approach to monitoring and enforcing the resilience requirements as providers work towards full compliance.

[redacted]