Ofcom
making communications work for everyone

Statement: General policy on ensuring compliance with security duties

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

Decision on guidance on resilience requirements imposed by or under sections 105A to D of the Communications Act 2003 (Ofcom's resilience guidance)

STATEMENT:

Publication date: 12 December 2022

Contents

Section

Published as separate annexes:

1. Overview

Following on from the requirement under section 105Y of the Communications Act 2003 (the '**2003 Act**'), we published a public consultation on 8 March 2022 setting out our proposed guidance on our general policy with respect to the exercise of our functions under sections 105I and 105M to 105V of the 2003 Act. We also proposed an update to our existing guidance on security requirements in sections 105A to D of the 2003 Act made necessary by the changes arising out of the Telecommunications (Security) Act 2021, so it focuses on how providers should approach their resilience obligations under the new framework. The consultation closed on 31 May 2022.

We received 28 responses. All non-confidential responses are published on our website.[1] After considering consultation responses, we are now publishing our final statement. A summary of the comments received and our responses to them are set out in Section 2.

[1] Consultation: General policy on ensuring compliance with security duties - Ofcom

What we have decided

We are publishing our statement of general policy under section 105Y of the 2003 Act regarding how we will exercise our new functions to seek to ensure that providers comply with their new security duties under the revised security framework.

Our statement explains the procedures that we generally expect to follow in carrying out our monitoring and enforcement activity. We are also providing general guidance about which security compromises we would normally expect providers to report to Ofcom and the process for reporting them.

A key objective of our monitoring role over the first few years of the regime is to determine if each provider is implementing appropriate measures with sufficient pace, as they continue to work towards full compliance. Where we find areas of concern, we will seek to work with providers to ensure appropriate and proportionate measures are implemented in accordance with the security duties. We expect this collaborative approach will foster more compliant behaviours and reduce the volume of breaches under the 2003 Act, as well as reducing the need for regulatory investigations. We will stand ready to engage our suite of enforcement powers as needed.

In addition, we are publishing our updated guidance on security requirements made necessary by the changes arising out of Telecommunications (Security) Act 2021.

The new security framework replaces existing sections 105A-105D of the 2003 Act, placing new security duties on providers of public electronic communications networks and services, both in the 2003 Act itself and in regulations. This is supplemented by statutory codes of practice which give guidance on the measures to be taken under sections 105A to 105D.

Given this new framework, we are updating our 2017 guidance on security requirements, in particular recognising that much of this guidance is no longer required given the Code of Practice that Government has published. In effect, this means that **we have decided to retain this guidance only insofar as it relates to the sub-category of security compromises relating to the resilience of networks and services, in terms of availability, performance or functionality.**

We have also taken this opportunity to update the guidance to take account of the revised framework, as well as to reflect the changing nature of resilience risks and Ofcom's experience of incident reporting and investigation.

1.1 The Telecommunications (Security) Act 2021 (the '**Security Act**')[2] introduced a revised framework for protecting the security and resilience of public electronic communications networks and services in the UK.

[2] Telecommunications (Security) Act 2021 (legislation.gov.uk)

1.2 The previous framework was set out in sections 105A-105D of the 2003 Act and complemented by Ofcom's guidance which was last updated in 2017 ('**Ofcom's 2017 Guidance**')[3].

Security duties and guidance under the revised framework

1.3 The new framework replaced sections 105A-105D of the 2003 Act and came into force on 1 October 2022[4]. It places new security duties on providers of public electronic communications networks and services ('**providers**'), including:

- the overarching security duties set out in the 2003 Act (sections 105A and 105C);
- duties to take specified measures imposed by the Secretary of State by regulations (sections 105B and 105D); and
- duties to report security compromises to Ofcom and to inform users (sections 105J and 105K).

1.4 The revised framework also provides for two forms of guidance for providers:

a) The Secretary of State's guidance on the measures to be taken by providers under sections 105A to 105D. The Secretary of State has powers to give such guidance by issuing codes of practice under section 105E of the 2003 Act;

b) Ofcom's general policy on how we will exercise our functions under sections 105I and 105M to 105V to seek to ensure compliance with the security duties. The 2003 Act (section 105Y) places a duty on Ofcom to publish a statement setting out such general policy and to have regard to it in exercising our relevant functions.

Ofcom's role

1.5 Ofcom has a general duty under section 105M of the 2003 Act to seek to ensure that providers comply with their security duties. This gives Ofcom a clear remit to work with providers to improve their security and monitor their compliance.

1.6 Ofcom also has certain reporting functions concerning security-related matters. In particular, Ofcom has a duty to inform the Secretary of State about certain risks of security compromise under section 105L, and also must prepare and send to the Secretary of State:

- security reports under section 105Z; and
- infrastructure reports under section 134A[5].

[3] Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003-2017 version; ofcom-guidance.pdf
[4] See The Telecommunications (Security) Act 2021 (Commencement) Regulations 2022.
[5] See, in particular, section 134B(1)(ha) and section 134B(2)(fa). In addition, Ofcom may prepare and publish additional reports under section 134AA of the 2003 Act.

DCMS consultation on the Regulations and the Code

1.7 As mentioned above, the Secretary of State has powers to impose specific security measures on providers by making regulations and give guidance on the measures to be taken by issuing codes of practice. In exercise of these powers, DCMS has:

- made regulations under sections 105B and 105D (the '**Regulations**')[6]; and
- published a code of practice under section 105E to give guidance for providers with relevant turnover in the relevant period of more than or equal to £50m (the '**Code**')[7].

Ofcom's procedural guidance

1.8 The revised framework gives Ofcom a general duty under section 105M of the 2003 Act to seek to ensure that providers comply with their security duties. To enable Ofcom to fulfil this role, the 2003 Act gives Ofcom powers to monitor and enforce industry's compliance with their security duties (sections 105I and 105N to 105V). In particular, it enables Ofcom to:

- require providers to provide information that Ofcom considers necessary for the purpose of carrying out its security functions (section 135, as amended by the Security Act[8]);
- direct providers to explain any failure to act in accordance with guidance given by the Secretary of State in a code of practice (section 105I);
- carry out, or commission others to carry out, an assessment of whether a provider is complying with the security duties (section 105N);
- give assessment notices (section 105O), including issuing an assessment notice which requires a provider to comply with a duty urgently (sections 105P and 105Q). Assessment notices may include requiring providers to complete system tests, make staff available for interview and permit persons authorised by Ofcom to enter operators' premises[9] to view information, equipment and observe tests;
- enforce compliance with the security duties (section 105S), including by imposing penalties (section 105T) and directing a provider to take interim steps (sections 105U and 105V).

1.9 Under section 105Y of the 2003 Act, Ofcom has a duty to publish a statement of their general policy with respect to the exercise of their functions under sections 105I and 105M to 105V of the 2003 Act. Annex 1 contains general guidance, given in the exercise of Ofcom's powers under sections 1(3) and 105Y of the 2003 Act, setting out how we plan to exercise our new powers.

[6] See The Electronic Communications (Security Measures) Regulations 2022 (S.I. 2022/933)
[7] Electronic Communications (Security Measures) Regulations and Telecommunications Security Code of Practice - GOV.UK (www.gov.uk)
[8] See, in particular, section 135(3)(iza)-(izc), section 135(3A)(za) and section 135(3C) of the 2003 Act.
[9] The 2003 Act (section 105R) places a duty on Ofcom to publish a statement in our annual report setting out the number of occasions on which premises have been entered pursuant to a duty imposed in an assessment notice.

1.10 In particular, our general statement of policy under section 105Y of the 2003 Act explains the procedures that we are generally expecting to follow in carrying out our monitoring and enforcement activity. It also provides general guidance about which security compromises we would normally expect providers to report to Ofcom and the process for reporting them. This guidance on providers' duties to report security compromises is intended to replace the incident reporting guidance which was set out in Ofcom's 2017 Guidance. In addition to the above, our general statement provides guidance about Ofcom's approach to sharing information with other public bodies, including DCMS, the National Cyber Security Centre (NCSC) and the Information Commissioner.

Ofcom's resilience guidance

1.11 The Security Act introduces the definition of a 'security compromise'. The guidance set out in Annex 2, which is given in the exercise of Ofcom's powers under sections 1(3) and 105Y, applies to the sub-category of security compromises relating to the resilience of networks and services, in terms of availability, performance or functionality (referred to hereafter as '**Resilience Incidents**').

1.12 Given the new framework described above, we are updating our 2017 Guidance, in particular recognising that much of this guidance is no longer required given the Government's new Code of Practice. Our updated guidance is set out in Annex 2. This guidance is intended to update the resilience-related guidance which was set out in the 2017 Guidance.

1.13 Ofcom's 2017 Guidance, insofar as it related to security compromises other than Resilience Incidents, has been superseded by the Code.

1.14 Ofcom's guidance on the reporting of security compromises (including Resilience Incidents) included in Ofcom's statement of general policy (set out in Annex 1) replaces Ofcom's 2017 Guidance about incident reporting.

1.15 The updated guidance now describes how we intend to use our powers and sets out the sources of guidance which we will consider when carrying out our functions in relation to resilience. It also provides some general observations and specific incident scenarios which will inform our approach to resilience. In recognition of this, we have recast what was general guidance as guidance on resilience requirements imposed by or under sections 105A to D of the 2003 Act. As and when Government decisions are made arising out of the UK Government's National Resilience Strategy Review, Ofcom would expect to review and update or revoke it as appropriate.

2. Responses to the consultation

2.1 We received a total of 28 responses to the consultation. All non-confidential responses are published on our website. We have set out a summary of stakeholder comments below, followed by Ofcom's response.

Procedural guidance responses

Compliance monitoring

Tiering

2.2 In the consultation (Annex 5, para 3.9), we proposed that our proactive compliance monitoring activities would be on providers in Tiers 1 and 2. We explained that this would be consistent with the approach taken in the Code and reflect our proportionate approach to compliance monitoring, balancing the need for security with the size and criticality of the networks and services involved.

2.3 *Tiering criteria* – VMO2 argued that our tiering criteria should be risk-based, not revenue-based, and a confidential respondent suggested that Ofcom should have regard to the differences between national and regional operators. We consider that a provider's relevant turnover can be seen as a proxy for risk, in the sense that if the networks or services of a larger provider are affected by a security compromise, this is likely to create a greater risk to the integrity of UK infrastructure, compared to the potential impact of a compromise affecting a smaller provider. A provider's relevant turnover can also be seen as a proxy for the size of its business, and therefore reflect its national or regional footprint. This approach is consistent with the DCMS response to their consultation on the Code (Part 2).

2.4 *Tiering notification* – Vodafone and Sky argued that it should be possible for Ofcom to notify providers of their tier faster than the proposed timescale of three months. Ofcom intends to complete this process as soon as practicable. In light of this comment, we have clarified in our procedural guidance (Annex 1, para 3.14) that we would expect to complete the process for establishing tiering by 1 January 2023, but it may take more or less time, depending on the information we receive from relevant providers.

2.5 *Introductory meetings* – In our consultation (Annex 5, para 3.13) we said we would seek to hold introductory meetings with Tiers 1 and 2 during the process for establishing tiering. Since most Tier 1 and Tier 2 providers have already consented to the use of the data they submitted as part of the annual administrative charges process for the purpose of establishing tiering, we consider that we no longer need to hold these meetings.

2.6 *Subsidiaries* – VMO2 sought clarification about how subsidiaries will be treated for the purposes of establishing tiering. Since using a provider's relevant turnover for tiering purposes has the benefit of minimising administrative burdens on providers because it is already applied by Ofcom in the context of determining the administrative charges,

providers should normally follow the same approach to reporting their relevant turnover for both purposes.

2.7 *Tier 3 and smaller providers* – Some respondents made comments about the approach to Tier 3 providers and smaller providers. Specifically:

a) FCS and INCA asked for further guidance for Tier 3 providers. We explain in our procedural guidance that any Tier 3 providers (or micro-entities) who do not hear from us can assume that they will not be part of the Tier 1 and Tier 2 compliance monitoring set out in that guidance (Annex 1, para 3.13). Given this, we do not consider that there is a need to give further guidance on the procedure we will adopt for our compliance monitoring activities. We will keep this position under review as the framework matures. We note that the Code provides that where a Tier 3 provider is a supplier of a Tier 1 or Tier 2 provider, the guidance in the Code concerning the supply chain duties will be relevant also to Tier 3 providers.

b) VMO2 expressed concerns about the lack of oversight of Tier 3 providers. We consider that we are applying an appropriate level of oversight of Tier 3 providers. While we do not expect to inform or meet with providers falling into Tier 3, as set out in our procedural guidance (Annex 1, para 3.13), Tier 3 providers are still required to comply with their legal obligations, and Ofcom could use its powers to investigate potential breaches and take enforcement action where necessary.

c) BUUK said that an additional tier (Tier 4) should be added to allow for an exemption to be provided to smaller companies in terms of potential enforcement action or the imposition of penalties on Tier 4. To the extent the BUUK argue that the substantive requirements should not apply to smaller companies, this is a matter for Government. We note that the Regulations provide that none of the security duties in the Regulations apply in relation to a network provider or service provider that is a micro-entity. To the extent that providers are not exempt, smaller providers are still required to comply with the security duties. Therefore, we do not consider it is appropriate to introduce a Tier 4. Although we are focusing our monitoring activity on Tier 1 and Tier 2 providers, Ofcom could still use its powers to investigate potential breaches and take enforcement action against smaller providers where necessary.

Information-gathering programme

2.8 In the consultation (Annex 5, paras 3.26-3.28), we proposed an information-gathering programme including an initial s135 notice (covering networks/services/assets in scope and an initial number of Code measures) followed by subsequent s135 notices issued at regular intervals of six or nine months.

2.9 *Early engagement* – Sky, Openreach and CityFibre expressed interest in early engagement with Ofcom. We accepted those suggestions and met with several providers over the summer to share with them an indicative draft of the type of questions that we would ask in our s135 notices, and sought initial comments from them.

2.10 *Formal vs informal information gathering* – VMO2 said that an "arms length" information gathering process would be time-consuming and inefficient, arguing that face to face engagement can be more productive than written answers. In Ofcom's view, formal (rather than informal) processes are needed to assess compliance. However, we intend to hold regular follow up meetings with providers, as set out in our procedural guidance (see the compliance monitoring approach flowchart in Annex 1, Figure 1 and para 3.29).

2.11 *Proportionality and timescales* – Several respondents (Neos Networks, TechUK, Verizon and two confidential respondents) expressed concerns about the potential burden on both industry and Ofcom, noting that Ofcom will receive a significant amount of information (which should not be underestimated) and that providers may receive also other s135 notices in parallel. VMO2 argued that we should extend the information request deadlines to six months for both Tiers 1 and 2, while KCOM said that Ofcom should take the size of providers into account, seeking a proportionate amount of information from smaller providers and allowing them more time to respond to information requests. BT said that Ofcom should update its guidance if DCMS chooses to align the Tier 1 and 2 timelines in the Code, while Verizon argued that s135 notices should only be issued after the relevant implementation period set out in the Code of Practice have elapsed. T confidential respondent said they were unclear if the proposed timescales were sufficient without seeing the s135 notices.

2.12 In light of stakeholders' comments, we have amended our procedural guidance (Annex 1, para 3.27) to allow six months for both Tier 1 and Tier 2 providers (instead of allowing only four months for Tier 1 providers, as initially proposed) to provide the required information. We have also aligned the frequency of our s135 notices, which we would expect to issue approximately every nine months to both Tier 1 and Tier 2 providers (instead of issuing one every six months to Tier 1 providers, as initially proposed). This is consistent with DCMS's decision to align the majority of the implementation timeframes set out in the Code for both tiers.

2.13 We also expect to take into account the extent to which we are already requiring information from the same providers. All information requests will be managed by our Information Registry, which we established in January 2020 to ensure we have a co-ordinated approach to gathering information. We also note, as a general point, that in accordance with s137(3) of the 2003 Act, Ofcom will ensure that any s135 notice is proportionate to the use to which we intend to put the required information.

2.14 We do not agree with the suggestion that s135 notices should only be issued after the relevant implementation period set out in the Code have elapsed, as this approach would not allow us to give an early warning of any potential compliance concerns, which is an objective of our monitoring process (see Annex 1, para 3.24).

2.15 As regards two confidential respondents' comments that they were unclear if the proposed timescales were sufficient without seeing the s135 notices, we note that the person holding the relevant information will normally have an opportunity to comment on both the information sought and the practicality of providing it in the given timescale. This is

because, as discussed below, we would normally expect to issue our s135 notices in draft form before issuing a final request.

2.16 *Draft requests* – Some respondents (BT, Openreach, Sky, Vodafone and a confidential respondent) emphasised the importance of issuing our s135 notices in draft form and allowing an opportunity to comment. In this regard, we confirm that we would normally expect to issue our s135 notices in draft form and offer an opportunity to comment. However, in line with Ofcom's general policy regarding its use of the statutory information gathering powers[10], in some cases we may consider appropriate to issue a notice directly in final form. For example, where an urgent investigation is required, or we issue the same information request as a previous one. In the latter case, our Information Registry would seek to provide respondents with notice of the planned request.

2.17 VMO2 asked how long providers will be given to comment on draft s135 notices. Where timescales allow, we expect that we would generally give 10 working days to comment on a draft notice issued as part of our regular monitoring programme, which is more time than the indicative period of three working days set out in Ofcom's general policy regarding its use of the statutory information gathering powers[11]. However, we may consider it appropriate to give a shorter or longer period, depending on the scale and complexity of the request, and the extent to which the same provider must respond to any other s135 notice in parallel.

2.18 *Associated facilities* – Cellnex suggested adding in our procedural guidance that Ofcom may seek information from a provider of "associated facilities". In light of this comment, we have clarified in our procedural guidance (Annex 1, para 3.22) that we expect to gather most of the information that we need to carry out our regular monitoring activity by issuing s135 information notices directly to the relevant providers of public electronic communications networks ('PECN') and public electronic communications services ('PECS'), but may also gather information from other relevant persons (s135(2)), such as persons making associated facilities available to the relevant providers, where we consider it necessary to carry out our functions.

Handling sensitive information

2.19 *Secure tools and systems* – Many providers[12] pointed out that Ofcom could become an attractive central point of information for potential threat actors and asked for more detailed information about how their data will be stored securely. In light of these comments, we have clarified in our procedural guidance (Annex 1, paras 3.30-31) that Ofcom plans to use an appropriate platform to securely process and store confidential information received from providers as part of the regime. This will enable us to manage, store and review information sent to us via a secure gateway. Operational arrangements

[10] Information gathering under section 145 of the Communications Act 2003 and section 13B of the Wireless Telegraphy Act 1949. Policy Statement (para 3.3).
[11] See footnote 10 above.
[12] TechUK, Sky, Neos Networks, Verizon and two confidential respondents

for providers to send us sensitive data in a suitably secure manner will be clarified as and when we issue such requests.

Reports to the Secretary of State

2.20 In our draft procedural guidance (para 2.12), we explained that Ofcom has certain reporting functions concerning security-related matters, including preparing and sending to the Secretary of State security reports under section 105Z and infrastructure reports under section 134A.

2.21 VMO2 and Vodafone were concerned that any sensitive or commercial information included in the reports prepared by Ofcom may get into the public domain, owing to a breach resulting in the report itself being made available to a third party, an FOI request or other reasons. These respondents suggested that: (i) any sensitive and confidential information in the security reports should be either redacted, anonymised (in a way that cannot be reverse engineered) or clearly marked as confidential (VMO2, p. 22); (ii) the infrastructure reports should be summarised at a level such that the potential disclosure to third parties would not further compromise the security of UK networks (Vodafone, p.7), ensuring that the granular details of security incidents are not disclosed (VMO2, p. 19) and (iii) any release of information should not disrupt the market, for example by naming and shaming network operators (Vodafone, p.7).

2.22 In relation to Ofcom's security reports under s105Z, these reports must include such information and advice as Ofcom consider may best serve the purpose of assisting the Secretary of State in the formulation of policy in relation to the security of public electronic communications networks and public electronic communications services (s105Z(1)-(2)), including the information about the matters listed in s105Z(4). Information shared with the Secretary of State under s105Z is exempt from the general restriction on disclosure under s393 (which prohibits Ofcom from disclosing such information without consent) by way of sub-section 393(6)(b).

2.23 As regards stakeholders' concerns about potential breaches arising from the process of sharing confidential information with the Secretary of State, we note that, in addition to using an appropriate platform to securely process and store confidential information, we will put in place operational arrangements with the Secretary of State to share any sensitive data in a suitably secure manner.

2.24 Once Ofcom has sent its report to the Secretary of State, it is for the Secretary of State to decide which information need to be excluded from publication or disclosure (s105Z(7)). If providers clearly mark which part of their response they consider to be confidential (providing reasons), we will pass this on to the Secretary of State and they can then consider which parts to publish or disclose.

2.25 In relation to VMO2's and Vodafone's concerns that individual providers would be named in our Ofcom's 'Connected Nations' reports, which in their view would have the potential for reputational damage or market disruption, Ofcom's intent is to publish information in aggregate or anonymous form, although we may refer to security compromises that are

already in the public domain. For the avoidance of doubt, information sent to the Secretary of State and published by Ofcom under sections 134A, 134AA and 134AB (i.e., information included in Ofcom's infrastructure reports or required for preparing such reports) is exempt from the general restriction on disclosure under s393 by way of sub-sections 393(6)(a) and (b).

2.26 In light of the comments above, we have amended our procedural guidance to clarify that nothing in section 393 of the Act limits, among others, the matters that may be published under section 134AB, or prevents the publication or disclosure of a report or part of a report under section 105Z(6) (Annex 1, para 7.5).

2.27 We have also clarified in (Annex 1, para 7.10) that we expect to adopt the same approach for the sharing of our security reporting with the Secretary of State as with our current infrastructure reports, namely to not notify providers of specific information that will be shared with the Secretary of State through the security report. We will however engage with providers where we propose to publish information related to compliance with security duties in our Connected Nations report. Therefore, our s135 information request will make clear that information gathered for our infrastructure and security reports could be shared with the Secretary of State without further reference to providers.

Risk-based approach

2.28 Vodafone said that Ofcom will need to take a "risk based" approach to assessing compliance given the high number of measures in the Code. This is broadly in line with our intended approach. Although we intend to gather information about the implementation of each of the measures in the Code (and any alternative or additional compliance measures a provider is taking), we will focus attention on areas of particular concern. In terms of enforcement, as set out in our Enforcement Guidelines, we cannot pursue every issue that comes to our attention and must weigh up the likely benefits of conducting an investigation against the resources required, and the comparative benefits of using those resources in other ways. The administrative priority matters we will generally consider are set out in paras 3.6-3.7 of our Enforcement Guidelines.

"Compliance journey"

2.29 TechUK and a confidential respondent questioned the concept of a "compliance journey" and regulation "ramping up over time", which we mentioned in our consultation (Annex 5, paras 3.5 and 3.10). We note that the burden of compliance with the security duties is expected to increase over time, in line with the phased implementation timeframes set out in the Code. We have clarified this point in our procedural guidance (Annex 1, para 3.10) by saying that "we see compliance as an ongoing journey, which will ramp up in line with the phased implementation timeframes set out in the Code".

Assessment notices

2.30 VMO2 asked when Ofcom expects to use assessment notices and what constitutes reasonable costs in relation to assessment notices. As set out in our consultation (Annex 5,

paras 3.41-3.42), the decision to issue an assessment notice is likely to indicate an escalation in our concerns around compliance that has not been resolved through routine engagement. Where appropriate, we may also use assessment notices to inform our enforcement activity. The 2003 Act requires providers to pay "the costs reasonably incurred by Ofcom" in connection an assessment under section 105N (s105N(2)(b)). Ofcom will decide what constitutes "reasonable costs" on a case by case basis.

Use of third parties

2.31 AMR CyberSecurity recommended that Ofcom considers the use of external providers to assess compliance, in line with the approach used for the Civil Aviation Assure scheme. Ofcom plans to generally use its own resources to carry out our regular monitoring programme for assessing compliance. However, in appropriate cases, we may exercise our power under s105N(1) to arrange for another person to assess compliance. We note, for example, that TBEST is carried out by independent third parties.

Further guidance and assurances from Ofcom

2.32 Some respondents sought further guidance and assurances from Ofcom. In particular, BT said it was unclear which provisions Ofcom will make to provide transparency to industry on its evaluations and developing policy thinking. It argued that Ofcom should continue to provide written feedback to market participants to facilitate the development of a common understanding of the requirements and drive good behaviours within the industry. VMO2 said there was a need for clearer guidance on how providers can demonstrate compliance, while Vodafone argued that Ofcom will need to "work collaboratively" with providers regarding alternative measures and technical solutions to the ones set out in the Code. CityFibre sought assurances that their "roadmap" would align with Ofcom expectations. The FCS argued that many of its members will need Ofcom to explain "what specifically they need to do to ensure compliance", suggesting that Ofcom considers a best practice security guide for all future networks, products and service developments.

2.33 We consider that, as with other areas of regulation of electronic communications networks and services, it is for each individual provider to interpret and act upon the obligations placed upon them. We do not intend to approve the compliance plans or roadmaps of individual providers. However, we may issue some additional high-level guidance as part of our supervisory approach, should we consider it appropriate. If we issue further guidance, we would normally expect to publish it on our website. For transparency, we also publish information on all open investigations on our website.

2.34 Neos Networks asked for more guidance on how they can demonstrate compliance, how Ofcom will measure performance (including certification) and what the consequences are of non-compliance, particularly if this is due to the "failure" of another provider. Ofcom is not running a certification scheme. The consequences of non-compliance will depend on each individual circumstance. Where a security compromise occurs or there is a risk of a security compromise occurring as a result of things done or omitted by third party

suppliers, Ofcom will consider (among other things) whether the primary provider has taken appropriate and proportionate measures to identify and reduce the risks of such compromise occurring, including by putting in place appropriate contractual arrangements and business continuity plans (as per Regulation 7 of the Regulations).

2.35 A confidential respondent asked Ofcom to clarify how providers which rely on a "host MNO" should demonstrate compliance. However, we cannot provide general guidance on this point as the evidence that providers will be expected to provide in order to demonstrate compliance will depend on the specific circumstances of each case.

"Comply or explain"

2.36 A confidential respondent asked for clarification on the types of circumstances where it could be necessary for a provider to give a statement confirming whether it is failing, or has failed, to act in accordance with the Code.

2.37 As set out under section 105I of the 2003 Act, Ofcom may direct a provider to give a statement where we have reasonable grounds for suspecting that the provider "is failing, or has failed, to act in accordance with a provision of a code of practice issued under section 105E". We may consider it appropriate to exercise this power where it is not entirely clear from the information gathered through our routine monitoring processes whether a provider is seeking to comply with its security duties through alternative measures. As stated in our guidance (Annex 1, para 3.37), we only anticipate using this power where we consider that a clear statement from a provider is necessary for us to consider whether further escalation might be appropriate.

Testing

2.38 In our consultation (Annex 5, para 4.14), we proposed that we would continue to run our penetration testing framework TBEST on a voluntary basis alongside our expanded powers.

2.39 *Testing criteria* – Several respondents[13] have raised questions about the criteria Ofcom intends to use to determine if alternative testing schemes to TBEST are acceptable, given that many providers already have alternative internal testing arrangements in place and/or face international compliance obligations. In our procedural guidance, we specifically refer to TBEST because it is a voluntary scheme which was already in place when the revised security framework came into force. Therefore, we considered it helpful to clarify that we do not expect to discontinue that scheme under the new regime. Although we note the high-level criteria for penetration testing set out in the Code (para 13.4), the approach that Ofcom will take to assessing any testing scheme which providers might wish to adopt does not fall within the scope of our consultation.

2.40 *Scope of testing* – TechUK asked Ofcom to commit to an open and collaborative approach on testing while a confidential respondent sought assurances that the scope of any test or audit will be agreed with the provider in advance. Ofcom would generally expect to involve

[13] BT, Openreach, VMO2, CityFibre, KCOM and a confidential respondent

the relevant provider in agreeing the scope of any test or audit. However, there may be circumstances where this is not appropriate.

2.41 *Providers in scope* – AMR CyberSecurity said that TBEST should be rolled out to lower tiers. TBEST is currently run under a voluntary basis and Ofcom continues to encourage all providers to undertake it to help identify all risks of security compromise. Comms Council UK sought clarity on Ofcom's approach to proportionality, pointing out that while the Regulations contain an exemption for micro-entities, Ofcom still has discretion to mandate testing on them through section 105O of the 2003 Act. We will take a proportionate approach to testing. As set out above, our monitoring activity will focus on Tier 1 and Tier 2 providers, but Ofcom could use its powers to investigate potential breaches and take enforcement action against smaller providers where necessary.

2.42 *Frequency of testing* – TechUK and a confidential respondent sought clarity on how often testing would be run, with TechUK suggesting a two to three yearly cycle. Although we note that the Regulations (Regulation 14) require providers to carry out, or arrange for a suitable person to carry out, such tests as are appropriate and proportionate "at appropriate intervals", the frequency of any such testing does not fall within the scope of our consultation.

2.43 *Equipment standards* – A confidential respondent supported setting transparent, objective standards for all equipment, irrespective of vendor. It argued that these should be based on international standards and best practices, to be assessed by recognised test laboratories (for example, the National Telecommunication Laboratory). We note that it will be the provider's responsibility to ensure that their equipment and configuration of equipment is appropriately tested, be this via their own testing or testing conducted by a third party.

2.44 *TBEST and the Code* – TechUK asked how TBEST will test against the full range of security requirements set out in the Code, such as supply chain security and SIM cards. Importantly however, TBEST does not identify and specifically test individual measures in the Code. TBEST takes a provider's security posture (including the measures it has taken to comply with the new security framework), along with its processes and culture. It tests the totality of all this to see how resilient it is against a well resourced cyber attack. So, depending on the scope of the TBEST, it may test all of, or only a subset of the security measures a provider has implemented, along with a provider's incident handling, security monitoring, employee compliance with security policies and other factors. As we explain in our procedural guidance (Annex 1, para 4.1), TBEST is a voluntary penetration testing framework which we will continue to run in parallel to Ofcom's use of its expanded powers under section 105N of the 2003 Act.

2.45 *CBEST* – TechUK expressed concern that TBEST is based on CBEST, which was built as an intelligence security testing regime for financial services. We note that while TBEST is derived from CBEST, it has been adapted for telecoms and it has worked well for the sector since its inception in 2018. NCSC are part of the intelligence services and are involved in TBEST as they were CBEST. However, in this capacity they are acting as the UK technical

authority for cybersecurity, with the objective of improving cybersecurity in telecoms providers.

2.46 *Sharing of TBEST reports* – A confidential respondent inquired how TBEST reports will be shared securely with NCSC and Ofcom and whether they would be subject to freedom of information (FOI). With TBEST, information is only shared between an identified and agreed closed group of organisations and named individuals within them. Ofcom is subject to the Freedom of Information Act 2000 ("FOIA"), meaning it has a general duty to provide access to information that is requested by a third party. However, as set out in the TBEST Handbook (which we will publish early in the New Year) it is likely that one or more FOIA exemptions will apply to a request for any confidential information provided to Ofcom for the purposes of TBEST.

Security compromise reporting Timescales

2.47 BT asked for Ofcom to provide clarity on the deadline for providers to have in place a system for reporting cyber incidents to Ofcom and significant risks of security compromises to users, setting this deadline at a reasonable period (i.e., at least 12 months) after commencement of the new regime. The legal requirements under sections 105J and 105K of the 2003 Act apply from commencement (1 October 2022). We have advised providers that they need to ensure they are ready to report any relevant incidents from 1 October 2022, in order to meet their legal obligations. We have also advised that where providers need to adjust their internal processes to meet our new procedural guidance, we would expect this would be done within a reasonable period following the publication of our final statement.[14] For further clarity, we would expect this to be phased in over the course of a few weeks to a couple of months, depending on the complexity of the provider environment and supporting processes in place for handling incidents.

End user reporting

2.48 In our consultation (Annex 5, para 5.4-5.7) we proposed that providers consider certain factors when determining whether users should be informed about a given risk of a security compromise. We also proposed factors that may make it appropriate to make either direct or indirect contact with the user.

2.49 *Proportionality* – BT, Openreach and Sky argued that reporting to users is disproportionate and raises security concerns, with BT suggesting that Ofcom should therefore give providers discretion over whether it is appropriate to send an alert. End user reporting is a legal requirement under s105J of the Act and therefore providers must comply with it. As set out in our procedural guidance (Annex 1, para 5.4), where providers have reasonable grounds for believing that a vulnerability within the network or service is unlikely to result in an actual security compromise, or even if it did, it would be unlikely to have an adverse effect on users, we would not expect users to be informed of such matters under section 105J. In our view, this should ensure that reporting to users is not disproportionate. In our

[14] See 'Update 20 April 2022' at Consultation: General policy on ensuring compliance with security duties - Ofcom

procedural guidance (Annex 1, para 5.5), we also specify factors that providers can consider when determining whether users should be informed.

2.50 *Providers in scope* – A confidential respondent asked how the legal obligation applies to providers who do not supply services to end users (e.g. wholesale altnets). We note that the duty in s105J refers, more generally, to any "persons who use the network or service and may be adversely affected by the security compromise".

2.51 *Consumer switching* – VMO2 expressed concerns about Ofcom's proposal that direct contact would be appropriate with users in instances where they could not mitigate the risk to themselves, but could move to another provider (Annex 5 to our consultation, para 5.6, third bullet point). VMO2 said this had the potential to cause confusion to consumers and serious reputational and commercial damage to providers. The notification obligation under s105J is intended to enable users to make informed choices about the security risks facing them and what they can do in response. Telling users there is a security risk facing them for which the provider has no reasonable mitigation to suggest may indeed cause reputational and commercial damage, but this should create incentives for the provider to avoid this outcome. Therefore, we have retained the text initially proposed at para 5.6 of our draft procedural guidance (see Annex 1, para 5.7), making a few minor changes for greater clarity.

2.52 *Industry roundtable* – BT, Sky and VMO2 noted the risks of inconsistent implementation by providers and urged Ofcom to set thresholds or set up an industry roundtable to secure some common standards for incident reporting. If industry can organise this, we would consider any further suggestions provided to Ofcom.

Reporting security compromises to Ofcom

2.53 In our consultation (Annex 5, Annex 1) we proposed a set of qualitative criteria and numerical thresholds that providers should take into account when considering whether to report a security compromise to Ofcom.

2.54 *Prepositioning* – Vodafone argued that reporting pre-positioning attacks (draft procedural guidance, para 5.14) would lead to over-reporting. We note that this reporting is not optional – it is required by the 2003 Act (section 105K(1)(b)). We encourage providers to talk to us where they have specific concerns.

2.55 *Cybersecurity-type compromises* – Several respondents (BT, Openreach, Sky, VMO2, Vodafone and TechUK) argued that Ofcom should provide clearer criteria for reporting security compromises related to cybersecurity, with respondents stressing that availability-based thresholds are not appropriate. Comms Council UK also asked what constitutes a "major" cybersecurity breach. In response to these stakeholders' comments, we have included a set of non-exhaustive, illustrative examples of cybersecurity-type incidents that we would normally expect to be reported, drawing on NCSC guidance (Annex 1, Section 5, Table 4), and changed "major" to "significant", in line with the wording in section 105K(1)(a) of the Act (Annex 1, para 5.19, bullet point 4). We have also clarified that the

availability thresholds relate only to the security compromises impacting service availability (Annex 1, para 5.19, bullet point 1).

2.56 *Urgent and "non major" security compromises* – A confidential respondent asked for clearer definitions for "urgent" incidents. Vodafone and two confidential respondents also considered a 3-hour deadline to report urgent incidents was unreasonable, suggesting 72 hours as an alternative. A confidential respondent argued that "non major" incidents should not be reported, while Vodafone asked for more guidance on what constitutes non-major incident. We have considered this feedback and in order to provide greater clarity, we have updated the text which describes "urgent", "non-urgent", and "non-major" security compromises and when each should be notified or reported to Ofcom (see Annex 1, paras 5.25-5.27). Regarding the 3-hour reporting deadline, we note this refers only to the initial notification of an urgent security compromise to Ofcom, rather than a structured report or root cause analysis which can be provided later.

2.57 *Number/proportion of users affected (mobile)* – Our draft procedural guidance (para A2.17) stated: "Where exact numbers are not available (for example due to a mobile cell site failure), we expect the provider to use historical data to estimate the number of end users affected." VMO2 asked for clarity on which mobile incidents to report, noting that the footnote referring to the reporting process between Ofcom and each of the four MNOs, which was mentioned in our 2017 Guidance (note 5, page 17) had been deleted. We have corrected this error by reintroducing an updated version of the relevant note which should address VMO2's concern (Annex 1, Table 2, note 4).

2.58 *Number/proportion of users affected (fixed)* – VMO2 pointed to similar issues on the fixed network in identifying number of customers affected, where a core transmission issue or a peering issue has led to some websites or services not being available for a subset of customers, but there is no overall loss of service. In relation to core transmission or peering issues affecting some customers, some services, or some internet destinations, we have updated our resilience guidance to clarify Ofcom's position (Annex 2, para 5.39).

2.59 *End users* – Comms Council UK asked what end users means in a business context, given the existence of resellers and complex supply chains. We recognise the challenges involved in identifying downstream customers and expect providers to identify reportable security compromises based on their own best estimate of the number of end users affected.

2.60 *Loss of a single technology* – According to para A2.10 of our draft procedural guidance, in the case of mobile incidents resulting in the loss of a technology (e.g. 2G, 3G, 4G or 5G) or service (e.g. voice, data) at specific cell sites, a full list of the affected sites should be provided. VMO2 asked us to remove that paragraph and sought clarity on the rationale for reporting incidents resulting in loss of a single technology, where service is maintained via another technology layer (e.g. "where 2G and 3G is unavailable but 4G is available"). We have retained such guidance (Annex 1, para 5.42) and note that the loss of a technology may impact users in different ways. For example, while 4G/5G phones will be backward compatible with 2G and 3G (while it is still live), some consumers still have devices which are 2G-only, 2G/3G-only, etc. Coverage may also vary slightly for 2G/3G/4G due to the frequencies and antennae used. Therefore, in the case of mobile connectivity, providers

should report any loss of network technology where the cumulative number of subscribers (across technologies where relevant) would exceed a threshold of subscribers impacted. For example, if 2G/3G circuit switched voice was lost, any customers with 2G/3G-only devices would lose service.

2.61 *Outages affecting the ability of a user to contact the emergency services* – In our draft procedural guidance (A1.3) we said that reportable security compromises included i) any security compromises affecting networks or services involved in connecting emergency calls (e.g. Call Handling Agent platforms, emergency call routing etc.) and leading to a reduction in the usual ability to answer or correctly route calls and ii) any security compromises that the provider is aware of that has a link to a potential loss of life. Comms Council UK said that this text made the fixed network numerical thresholds in Table 1 redundant. We note, however, that the two references are complementary; the first relates to the services involved in connecting emergency calls, not individual customer connectivity (which the thresholds in the table relate to).

2.62 *Mobile roaming* – Our draft procedural guidance (Annex A1, note 2 to Table 2) contained the following exemption: *"Where a provider expects emergency roaming will have allowed customers in the affected area to retain 112/999 access, it is not required to report the incident under this threshold"*. Vodafone argued against including such exemption for emergency roaming. In light of Vodafone's comment and given the technology evolutions and interworking complexities (3G switch-off, 4G LSS/VoLTE, 5G-SA LSS/VoNR) and associated changes in coverage for different radio types, network capabilities, and device capabilities, we have decided to remove this exemption.

2.63 *Broadcast incidents* – VMO2 asked whether broadcast incidents needed to be reported. Broadcast network infrastructure which comprises a transmission system for the conveyance of signals is an "electronic communications network", and broadcast services having as their principal feature the conveyance of signals are an "electronic communications service", except insofar as they are a content service (s32(2) of the 2003 Act). Therefore, we have added the thresholds for reporting security compromises affecting "Broadcasting service/network for reception by the general public" which were set out in Ofcom's 2017 Guidance (Annex 1, paras 4.19-4.10 and Table 3).

2.64 *Media coverage* – In our draft procedural guidance (para A1.1), we said that "security compromises attracting national mainstream media coverage" should be notified as "urgent". A confidential respondent said that it does not believe "media" should be a qualitative criterion because it is unclear what should be included. Comms Council UK asked for more clarity on what constitutes national mainstream media coverage and trade news sources. TechUK also said that such qualitative criterion is harder to build into any automated reporting system. The reference to "national mainstream media coverage" is intended to be illustrative only and is one of several qualitative criteria in our procedural guidance. By way of example, a compromise attracting the attention of BBC journalists would normally meet this criterion. For clarity, we have updated the guidance (Annex 1, para 5.25) to reflect that those security compromises attracting national mainstream

media coverage should be notified as urgent regardless of whether they meet the quantitative thresholds in Tables 1, 2 and 3.

2.65 *Wholesale fixed and mobile services* – Comms Council UK said Ofcom may wish to be cautious about including "any single security compromise that affects the provision of wholesale services to both fixed and mobile communications providers" as one of the qualitative criteria for urgent incidents, given that it may lead to over-reporting. We have updated the guidance (Annex 1, para 5.25, final bullet point) to clarify that we only intend for these compromises to be notified as urgent where they are likely to affect the provision of wholesale services to both fixed and mobile communications providers in a given geographic area.

2.66 *Data breaches* – VMO2 asked what data breaches it must report to Ofcom and how Ofcom proposes to work with the Information Commissioner in relation to investigation and enforcement of personal data breaches. Providers must report data breaches to Ofcom only if they meet the definition of "security compromise" set out in s105A(2)-(3) and the reporting criteria set out in s105K of the 2003 Act. The Information Commissioner and Ofcom have signed a Memorandum of Understanding, which establishes a framework for cooperation and information sharing between the two organisations[15].

2.67 *Duplication of reporting* – Verizon and TechUK argued for a streamlined approach to prevent duplication of reporting to the Information Commissioner under the Network and Information Systems Regulations and the UK General Data Protection Regulation. TechUK's proposal was that providers should report all incidents to one regulator, who would then be responsible for sharing and disseminating info to others. Providers' duties to report incidents under the 2003 Act (s105K), the Network & Information Systems (NIS) Regulations and the UK General Data Protection Regulation (GDPR) are separate reporting obligations set out in law. Where providers are required to report an incident to both Ofcom and the Information Commissioner, one practical solution would be to send one email to both organisations.

2.68 A confidential respondent asked for "use cases" for security compromises which are reported to other Government agencies and therefore reportable to Ofcom. We consider that the NCSC and the ICO are two key examples. KCOM said that the duty to inform Ofcom of information shared with NCSC/ GCHQ is likely to have "a chilling effect" on willingness to share information. We note that if a security compromise meets the criteria set out in s105K, providers are required to report them to Ofcom (regardless of whether providers have also proactively informed NCSC/GCHQ).

2.69 *Data retention (period)* – In line with Ofcom's 2017 Guidance (para 4.12), in our draft procedural guidance (para 5.25) we proposed that providers should keep data for security compromises that have been reported for no less than 18 months following incident resolution. VMO2 questioned the length of this retention period, pointing to the minimum period of 13 months set out in Regulation 6(3)(e) of the Regulations. In light of this

[15] https://www.ofcom.org.uk/about-ofcom/how-ofcom-is-run/organisations-we-work-with

comment, we have decided to shorten the data retention timelines from 18 months to 13 months, noting that a period of 13 months would be consistent with the retention period set out in regulation 6(3)(e).

2.70 *Data retention (scope)* – VMO2 also sought confirmation from us that only the data collated for the purposes of incident reporting and further discussion with Ofcom should be retained, but not the underlying data stored in network systems. We expect providers to hold information submitted in their incident reports as well as relevant underlying data for the 13 month period.

Enforcement

2.71 In our consultation (Annex 5, Section 6), we set out how we generally expect to exercise our enforcement powers, including our power to impose penalties (section 105T) and our power to direct a provider to take interim steps (sections 105U and 105V). We noted that our procedural guidance in relation to our powers under the security framework should be read alongside Ofcom's Enforcement Guidelines and Ofcom's Penalties Guidelines.

2.72 *Proportionality* – A confidential respondent stressed the need for proportionality in Ofcom's approach, while Sky sought greater clarity about the criteria which Ofcom intends to apply in deciding when to initiate formal enforcement action. As explained in Ofcom's Regulatory Enforcement guidelines[16], which apply to our enforcement under the security framework as well, Ofcom seeks to take enforcement action: a) in an efficient and effective way; b) that is evidence-based, proportionate, consistent, accountable and transparent; and c) that is targeted only at cases where action is needed. The administrative priority matters that we generally consider in deciding whether to open an investigation are also set out in Ofcom's Regulatory Enforcement Guidelines (paras 3.6-3.7).

2.73 *Collaborative approach* – TechUK and Sky encouraged Ofcom to engage and collaborate with providers as soon as possible, to minimise the risk of "unnecessary and counterproductive formal enforcement action". We will engage with providers as we normally do for any potential enforcement activity. Ofcom takes a pragmatic and collaborative approach to enforcement. Co-operation is something we do take into account when we impose penalties.[17]

2.74 *Discussion with Ofcom* – Openreach asked for further discussion with Ofcom on its new powers, especially where they are not covered by the Enforcement Guidelines. We note that we have consulted stakeholders on our approach to exercising our new powers as part of our consultation on Ofcom's General policy on ensuring compliance with security duties and our consultation on "Ofcom's approach to enforcement" (Consultation on revising the Regulatory Enforcement Guidelines, paras 3.6-3.8). However, we welcome further discussion with providers.

[16] https://www.ofcom.org.uk/__data/assets/pdf_file/0028/249094/statement-revising-enforcement-guidelines.pdf
[17] Penalty guidelines, para 1.12.

2.75 *Powers of entry* – A confidential respondent asked for more clarity on when Ofcom would use its powers of entry, while another confidential respondent wanted confirmation that Ofcom will follow the Home Office's Code of Practice on powers of entry. To exercise our power of entry, we need to issue an assessment notice. As set out in our procedural guidance (Annex 1, paras 3.45-3.46), the decision to issue an assessment notice is likely to indicate an escalation in our concerns around compliance that has not been resolved through routine engagement. Where appropriate, we may also use assessment notices to inform our enforcement activity. As set out in our procedural guidance (Annex 1, para 3.50), we will have regard to the Home Office Code where relevant.[18] This approach is consistent with s51(1) of the Protection of Freedoms Act 2012.

2.76 Cellnex suggested adding that Ofcom may exercise its power of entry by issuing an assessment notice to the manager of a facility used by more than one provider as well as to the provider concerned. Our powers to give assessment notices are only in respect of providers of public electronic communications networks ('PECN') or public electronic communications services ('PECS'). However, where a provider has a right of access to premises owned by a third party (for example, under a letting agreement), we can request the provider to permit an Ofcom's employee or a person authorised by Ofcom to enter such premises.

2.77 *Information notices* – A confidential respondent asked for clarification on the definition of 'failure to comply' with a s135 notice. As set out in our Enforcement guidelines (paras 4.13 to 4.16), Ofcom's statutory information gathering powers are a critical tool in obtaining the information necessary to assess compliance and where necessary take appropriate enforcement action in the interests of citizens and consumers. We expect recipients to provide accurate and complete information in response to statutory information requests by the given deadline.

2.78 *Interim steps* – Openreach asked for more detail on timescales of the three-stage process for directing providers to take interim steps. In our consultation (Annex 5, para 6.9), we summarised the process for Ofcom's power to direct providers to take interim steps (sections 105U and 105V), which involves: 1) giving a notification setting out the interim steps proposed by Ofcom (section 105U), 2) allowing the provider an opportunity to make representations (section 105V(1)(b)) and 3) issuing a direction to take interim steps (section 105V). Our Enforcement Guidelines give further information about the standard steps Ofcom goes through in opening and pursuing an investigation. Beyond this, it is not our practice to give any further details on timings of the enforcement process. However, as we say in our procedural guidance (Annex 1, para 6.19), "the time given to make representations under section 105U(2)(C) is likely to be short".

[18] For the avoidance of doubt, the guidance provided in the Home Office Code is relevant to the exercise of Ofcom's powers of entry only is so far as it is consistent with the statutory framework. For example, the guidance in the Home Office Code about giving advance notice or conducting an unannounced inspection (paras 8.1-8.5) is not relevant to the exercise of Ofcom's powers of entry because s105O(7)-(8) and s105P(3) of the Act do not allow unannounced inspections and require Ofcom to give an advance notice of at least two months (or 14 days in urgent cases).

2.79 *Customer impact* – A confidential respondent said that, alongside the opportunity for providers to submit representations, they would also welcome the opportunity to "demonstrate controls and mitigation of any customer impact", so Ofcom can factor these into their decisions. As set out in our Enforcement Guidelines (para 5.2, 5.14 and 5.17), we will give providers the opportunity to give both written and oral representations. There is nothing to specify what information a provider can, or cannot include in those oral and written representations.

2.80 *Civil liabilities* – VMO2 sought more clarity on Ofcom's consent as it relates to civil liability. Section 105W ("Civil liability for breach of security duty") requires Ofcom's consent to be obtained before legal proceedings are brought in respect of breaches of security duties. This point is covered in our Enforcement Guidelines (see, in particular, paragraphs 10.1-10.12).

Information sharing

2.81 In our consultation (Annex 5, para 7.6), Ofcom explained that we may need to share information with other bodies on an ad hoc basis, such as the Information Commissioner's Office (ICO), to enable them and Ofcom to perform their respective functions.

2.82 *Providers' consent* – Sky, VMO2 and two confidential respondents sought assurances that information would not be shared without their consent. As set out in our procedural guidance (Annex 1, section 7), Ofcom will seek consent from providers where appropriate. However, some statutory gateways, including those set out in section 393(2) of the 2003 Act, enable the sharing of information without consent. In the context of the exercise of our network security functions under the 2003 Act, we anticipate in certain circumstances disclosing information gathered under the Act with other persons (in particular, DCMS and NCSC) under relevant statutory gateways without further reference to the provider. Where we take this approach, we would expect to inform providers of the fact that we have disclosed such information to another person, but only to the extent that timescales allow and we consider it appropriate to do so.

2.83 We have made a few changes to our draft procedural guidance in order to clarify our approach. In particular, we explain that for security and infrastructure reporting to the Secretary of State, the disclosure to the Secretary of State and NCSC of security compromises reported to Ofcom under section 105K and the disclosure of information to NCSC where this is necessary for the exercise of their functions, we expect to disclose the relevant information without prior reference to the provider (Annex 1, paras 7.7 - 7.13). We will also explain the approach we intend to take in any s135 notices requesting information.

2.84 *Pre-approval process* – Openreach suggested drawing from the pre-approval process for Connected Nations for sharing the information gathered by Ofcom. The process to which Openreach refers applies to the sharing of data where an information disclosure gateway does not apply and therefore, provider's consent is required. We do not consider that this process would be appropriate for the disclosure of data under a statutory gateway. Where

a similar need is identified going forward under the security regime in respect of ad-hoc sharing of data, we may consider a similar approach.

2.85 *Information management policy* – Vodafone argued for a comprehensive information management policy to be put in place, including what information is released and to whom; 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. We note that any information management policy will be internal to Ofcom and we will not be sharing the detail of this with stakeholders.

2.86 *Keeping industry informed* – The FCS asked whether Ofcom will publish a list of providers who are found to be compliant in order to enhance confidence in those providers. We do not plan on publishing any such list. It also asked whether, where security issues are identified, the whole tier chain will be informed in a timely manner, and the issue made public to enhance awareness, increase confidence and enable users of any services impacted to be kept informed. We note that Ofcom's exercise of its powers under s105L will depend on the specific circumstances of each case.

2.87 *Duty to inform the Secretary of State* – VMO2 stressed the need for Ofcom to exercise caution in fulfilling its duties under s105L. For the avoidance of doubt, the disclosure of information under section 105L does not require Ofcom to obtain consent from the relevant person (section 393(6)(aza) of the 2003 Act). As mentioned above, we anticipate in certain circumstances disclosing information gathered under the 2003 Act with other persons (in particular, DCMS and NCSC) under relevant statutory gateways without further reference to the provider. These circumstances include the disclosure of information under section 105L to the Secretary of State. However, where timescales allow and we consider it appropriate, we may inform providers of the fact that we have disclosed such information to the Secretary of State.

2.88 *Further clarifications* – As discussed above, we have also added a couple of clarifications at paras 7.5 and 7.7 - 7.13 of our procedural guidance in light of stakeholders' comments.

Resilience guidance responses

Additional guidance

External guidance

2.89 Sky and VMO2 were unclear over the legal status of the additional sources of guidance that Ofcom cited in the consultation. A confidential respondent said it would be disproportionate to ask providers to follow the ENISA guidelines as well as the NCSC's CAF framework. They said this concern would be exacerbated should the two documents diverge in their guidance. As set out in our resilience guidance (Annex 2, para 4.9), the documents to which Ofcom refers in paras 4.15 – 4.21 are best practice that we expect providers to consider where relevant to their operations, but there is no legal obligation to follow them.

Guidance from Ofcom

2.90 VMO2 asked for further guidance on how providers can demonstrate compliance as well as practical advice on implementation and compliance, while INCA encouraged Ofcom to engage with all providers on an ongoing basis with regards to the interpretation of the very "high level and general provisions". Mid Deeside Community Council also said that Ofcom's proposed approach is not detailed enough and relies on the provider to identify and mitigate the risks.

2.91 The Telecommunications (Security) Act 2021 (which removes the previous sections 105A-D of the 2003 Act and replaces them with strengthened security duties) introduced the definition of "security compromise". This definition includes a sub-category of compromises relating to the resilience of networks and services, in terms of availability, performance or functionality (referred to in our resilience guidance and this document as "Resilience Incidents").

2.92 Ofcom's 2017 guidance, insofar as it relates to security compromises other than Resilience Incidents, has been superseded by the Code of Practice issued by the Secretary of State under s105E. In effect, this means that we have retained our 2017 guidance only in so far as it relates to Resilience Incidents. We have also updated this guidance to reflect the changing nature of resilience risks and Ofcom's experience of incident reporting and investigation.

2.93 At this time, Ofcom is not publishing any further guidance relating to resilience in addition to our updated resilience guidance. However, Ofcom will continue to work with government and industry to monitor the reliability of electronic communications networks and services and the resilience landscape. In particular, as and when Government decisions are made arising out of the UK Government's National Resilience Strategy Review, Ofcom would expect to review and update or revoke our resilience guidance as appropriate. As set out in our resilience guidance (Annex 2, para 2.11), we may also make further revisions to it from time to time, such as to reflect the introduction of further codes of practice under s105E by the Government.

Public access to emergency services

2.94 In our draft resilience guidance (para 5.31-5.34), we referred to the requirements set out in General Condition A3 regarding access to emergency services and provided guidance on the test calls that we would normally expect providers to conduct when they conclude any change management activity with potential to affect access to the emergency services. We also noted that BT, the current provider of Emergency Services Access call handling centres, had developed a set of test call handling procedures and Ofcom is publishing an outline of these procedures on Ofcom's website in parallel with our resilience guidance[19].

2.95 VMO2 said that it agreed in principle with those requirements but asked for additional clarity on exactly what is expected, appropriate and proportionate in order to comply. In

[19] https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/telecoms-industry-guidance

particular, it requested a copy of BT's test call handling procedures as soon as possible. Ofcom is publishing an outline of these procedures on Ofcom's website in parallel with our resilience guidance.

2.96 VMO2 also asked for confirmation that the requirements set out in paras 5.31-5.34 in our draft resilience guidance would begin on the commencement date (i.e., from 1 October 2022). For the avoidance of doubt, while the relevant duties under the security framework came into force on 1 October 2022, the requirements set out in GC A3 were already in force before the introduction of the revised security framework and will continue to apply in parallel with the new regime.

Ofcom's role

2.97 TechUK and Vodafone have encouraged Ofcom to drive industry positions on resilience of interconnection, resilience of access networks, and power resilience. Mid Deeside Community Council said further consideration needed to be given to power resilience, given the impact prolonged power outages can have on access to communications.

2.98 Ofcom is working on resilience of interconnection. The work with NICC on SIP Overload Controls is an example of that. Although the overarching duties set out in sections 105A and 105C of the 2003 Act apply in relation to any security compromises (including those relating to the resilience of networks and services), the focus of the more detailed duties set out in the Regulations and the technical guidance measures in the Code is mainly (but not exclusively) on cybersecurity, rather than other forms of resilience. Beyond the scope of the new security framework, we will continue to work with government and industry on the broader topic of network and services resilience and reliability.

2.99 Ofcom is actively engaged in discussions related to the interdependencies between telecommunications and power with the Power Resilience working group in the EC-RRG as well as with the ENA, Ofgem and HMG.

Proportionality

2.100 A confidential respondent said that the resilience measures would benefit from being more straightforward and less prescriptive and recognise industry expertise in tackling resilience issues, being at the forefront of risk identification and management. KCOM argued that Ofcom should ensure that the various factors which Ofcom proposes to take into account in relation to resilience are consistent and practicable, stressing that providers cannot reasonably be expected to comply with conflicting, unreasonable, dangerous or impossible requirements. The FCS stated that any resilience requirements should be "appropriately targeted on the capability owner and linked to the appropriate risk".

2.101 Proportionality forms part of the legal framework in that sections 105A and 105C of the 2003 Act require providers to take such measures as are "appropriate and proportionate". Fundamentally, all providers of public electronic communications networks and services should consider the networks and services that they provide and how those services may be used in relation to resilience and reliability expectations of the customers of those

services. Generically, resilience requirements are based on the kinds of services offered to customers, rather than the capabilities of the provider.

Resilience of legacy networks

2.102 TechUK and two confidential respondents sought further information on Ofcom's planned approach to legacy networks. Ofcom appreciates the challenges of operating legacy networks that are beyond their original planned lifespan and changes in customer needs and behaviours enabled by new technologies. However, the guidance in paragraph 2.6 of the Code makes clear that it would not be appropriate for providers to disregard the resilience of networks based on what may or may not happen to them in the future.

2.103 We also note that our resilience guidelines have not significantly changed since the 2017 Guidance. Therefore, providers should have been working to meet our resilience expectations for many years now.

International considerations

2.104 A confidential respondent said there was a need to ensure Ofcom explicitly acknowledge the multiplicity of valid business models and consider the challenges of providing international customers with a seamless global service. Ofcom does consider challenges of providing international services. However, if an operator provides services in the UK, it must ensure compliance with the relevant UK regulatory framework.

Supply chain and outsourcing

2.105 Our draft resilience guidance (paras 5.14-5.17) retained the guidance on supply chain and outsourcing already contained in the 2017 Guidance (paras 3.20-3.22) and referred to the supply chain duties in the Regulations (Regulation 7).

2.106 Sky asked Ofcom to offer more specific guidance on issues related to the supply chain. These include more clarification on i) the criteria for supplier engagements to be considered resilience risks about which providers should seek early engagement with Ofcom; ii) at what stage of the procurement cycle a provider should seek engagement; and iii) timeframe for a response be provided following any engagement.

2.107 Regarding the criteria for supplier engagements, it is for providers to judge in the context of their networks/services and planned use of a new supplier where a significant resilience risk could arise. However, we welcome discussion with providers if they are unsure. As and when high-risk vendor (HRV) restrictions apply to any given supplier, the provider should consider whether use of that vendor within the scope permitted under the relevant designated vendor direction is creating any additional resilience risks. Regarding timeframe, our resilience guidance (Annex 2, para 5.17) states that we strongly encourage providers to discuss with us at an early stage any planned new arrangements that may have significant resilience implications.

Shared facilities

2.108 Cellnex proposed some additions to specially refer to such cases where providers sharing a common facility have agreed a common security standard. We have decided not to make these changes because the existence of any such common security standard would not excuse providers from their security duties under the 2003 Act, including those relating to network and service availability, performance, and functionality. This is because, as set out in our resilience guidance (Annex 2, para 5.53), a provider cannot contract out of its statutory obligations.

Non-compliance by third parties

2.109 In our draft resilience guidance (para 5.53), we retained our previous guidance on outsourcing to third parties (para 3.52 of the 2017 Guidance) and provided further guidance on the types of controls over third parties that we would normally expect providers to take. Sky argued that Ofcom needed to clarify its approach in relation to non-compliance by third party suppliers. We do not consider it necessary to provide further guidance on this topic. Our resilience guidance (Annex 2, para 5.53) makes clear that a provider cannot contract out of its statutory obligations. Therefore, the obligations on a communications provider to comply with their statutory obligations (related to 'resilience') continue to remain their responsibility regardless of any outsourcing arrangements.

Vendor diversification

2.110 A confidential respondent expressed concern over the absence of any requirement for supply chain or equipment vendor diversification in our resilience guidance, given that diversity of suppliers is critical for the long-term health of public telecommunications networks in the UK. However, we note that supply chain vendor diversification does not fall within the scope of our consultation on updating our resilience guidance.

Protecting end users – risk assessment and provision of information

2.111 In line with our 2017 Guidance (para 3.35), we said in our consultation (draft resilience guidance, para 5.23) that providers are expected to provide information about the resilience of their services to allow customers to make informed purchasing choices.

2.112 Sky, VMO2, INCA and two confidential respondents said that there is a lack of clarity around Ofcom's expectations in this area and asked for Ofcom to provide more practical advice and examples of the type of information providers would need to give users. Sky and a confidential respondent stressed that, as currently worded, the requirement could be met in varying different ways by different providers, reducing the ability of end users to make informed decisions. Furthermore, INCA argued that making too much architecture and network design information public could have the adverse effect of increasing risk and reducing overall resilience.

2.113 We do not consider it necessary to provide further advice on this matter, noting that we are just retaining guidance that has been in place for a number of years. In our view, the provision of resilience-related information would increase transparency and help end users making informed decisions, even though information could be provided in different ways.

Interconnection

2.114 In our draft resilience guidance (paras 5.26-5.27), we said that we will use ND1643 and ND1653 as reference points when determining if a provider has taken appropriate measures.

2.115 VMO2, Vodafone, Comms Council UK and two confidential respondents expressed concern in relation to the reference of ND1653. In particular, some providers argued that implementing ND1653 is not practical due to the logistics and timing required to implement it. At the time of publication of this statement, NICC is updating its guidance related to SIP Overload Controls for network interconnections in a new NICC specification (NICC ND1657). As such, we have omitted references to ND1653 in our resilience guidance and added that it is likely that Ofcom will use the future NICC ND1657 guidance on SIP Overload Control as a reference (Annex 2, para 5.27).

Security compromise reporting

2.116 Several stakeholders asked for more clarity in relation to what they will need to report to Ofcom. In particular, they asked for more clarity in relation to which compromises would be reportable (VMO2), as well as further examples of incidents with a significant impact (a confidential respondent) and the type of evidence which is likely to be relevant (a confidential respondent)." In light of these comments, we have decided to add some illustrative examples of reportable cybersecurity incidents in the procedural guidance. The procedural guidance also contains thresholds related to fixed and mobile services impacts in terms of number of users and duration.

2.117 The main purpose of updating our resilience guidance was to align it to the new security framework. In future updates, we will consider providing further examples of evidence that is likely to be relevant in relation to some types of incidents. We note that some examples of resilience-type compromises are already set out in our updated resilience guidance (see page 16 onwards).

Governance

2.118 VMO2 recommended setting up a best practice industry group or an NICC standards task group to support providers with delivery and governance against the Act, Regulations, Code and procedural guidance. Ofcom welcomes providers to set up best practice industry groups.

Other matters

2.119 An individual argued that the proposed guidance is not written in plain English and would not be widely understood. We endeavour to write all Ofcom documents in plain English. However, the nature of the subject matter means we need to include technical and legal language.

2.120 Respondents also made several comments on issues which fall outside the scope of our consultation, mostly on how aspects of the Code will apply. These included the following:

- How the legal framework applies to "novel services" on a standalone basis (for example, providers offering eSIMs or 'over-the-top' services which interconnect with the PSTN);
- Whether and how application providers (for applications such as Teams/Zoom etc.) should ensure the compliance of the applications they supply;
- The applicability of the Code to legacy networks;
- How providers with a global footprint should demonstrate compliance alignment with international security standards;
- Treatment of joint ventures;
- Concerns about the "localisation measures" in the Regulations, such as Regulation 5(3)
- Application of the Supply Chain requirements in 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 Regulation 3(1)(b) to the growth of existing networks;
- Whether it would be acceptable to address resourcing challenge of implementing the framework by recruiting staff at other offices within or outside the EU

2.121 Where comments relate to the Code, further information can be found in DCMS's response to their public consultation[20]. For example, joint ventures and legacy networks are discussed in Part 1 (under the section entitled *"Supply chain - proposed exemption for joint ventures and third party networks"*) and Part 4 (*"Legacy networks and services"*) of DCMS's response.

[20] DCMS proposals for new telecoms security regulations and code of practice – government response to public consultation