Ofcom

making communications work
for everyone

Review of Security Guidance

Consultation on updating Ofcom’s guidance on security requirements in sections 105A to D of the Communications Act 2003

Consultation

Publication date:	30 June 2017
Closing Date for Responses:	7 September 2017

About this document

This consultation document seeks views on changes we propose to make to our published guidance for telecoms providers about security.

Companies that provide public communications services and networks are required to take steps to ensure their offerings are secure and reliable. In particular, they need to ensure end customers are protected in the event of any security problems, and that networks are resilient to such problems or equipment failures, and can continue to operate. They also must report any significant security incidents to Ofcom.

We are responsible for investigating, and where necessary penalising, companies if these requirements are not met. To assist companies in understanding what is expected of them, we publish high level guidance setting out what we will take into account when deciding if a company has complied with its obligations. The guidance also explains the process for reporting incidents and what we view as the threshold for a “significant” incident.

Our guidance was originally published in 2011, when the security obligations first came into force, and we revised it in 2014. We keep the guidance under continuous review, and think it is now time to update it again. The threats to the security of communications services have changed somewhat over the last three years and hence the guidance we provide on how to address them needs to change accordingly. We also propose revising some of our guidance on incident reporting, and providing more information about how we will use our powers in the event we need to investigate or take enforcement action.

The consultation period will run for 10 weeks following the publication of this document. During that time, we would welcome written submissions from anyone with an interest in the issues raised.

Contents

Section | Page

Annex | Page

Section 1

Introduction

1.1 Telecoms services are an essential part of a modern economy and society. Some of the underlying networks that deliver them are part of the critical national infrastructure. This means that their loss or compromise has been judged by Government as likely to result in severe economic or social consequences, or to loss of life. For many other infrastructure sectors, such as energy and finance, telecoms provide an essential input to allow them to continue functioning. That providers take effective measures to protect the security and reliability of their services and networks is therefore vital to customers and to the UK economy as whole, as well as to the providers themselves.

1.2 The legislation governing telecoms regulation reflects this. It imposes statutory obligations on providers of public electronic communications networks and services (to which we will refer collectively as communications providers (or CPs) throughout this document) to manage security and reliability appropriately and requires them to report significant incidents to us at Ofcom. When these obligations initially came into force in 2011, we published high level guidance for CPs on how we would approach any compliance investigation. We reviewed and updated this guidance in 2014[1] to reflect changing threats and vulnerabilities, additional experience from implementing the requirements, and to incorporate feedback from stakeholders. We explained at the time that we expected to continue updating the guidance from time to time.

1.3 We keep the guidance under continuous review, and believe the time is right to update it again. This consultation sets outs the changes we are proposing to make and our reasoning for these changes. We would welcome stakeholders' views on whether these changes are appropriate, and whether there are other things we should address in the revised guidance.

1.4 The current version of the guidance was significantly restructured and simplified compared to the original version. For the current review, we do not propose to alter the overall structure, but instead to update or add to the existing text in a number of areas. The main areas, none of which are new, in which we propose changes or additions are as follows:

- **Cyber security** – make it explicit that we consider taking appropriate steps to manage cyber security risks to be an essential part of a CP's compliance obligations. Explain that we will look to detailed guidance and best practice from elsewhere, such as the National Cyber Security Centre[2], when considering the appropriateness of actions taken by a CP.

- **Risk management and governance** – emphasise the importance of effective governance within CPs, and add additional guidance in relation to our approach to security standards and the management of outsourcing.

- **Incident reporting** – address concerns that there is a lack of consistency in the reporting of incidents among mobile network operators, and formalise the process for timely reporting of the most major incidents.

[1] https://www.ofcom.org.uk/__data/assets/pdf_file/0021/51474/ofcom-guidance.pdf
[2] https://www.ncsc.gov.uk/

- **Maintaining network availability** – emphasise the need to take appropriate steps to avoid single points of failure and manage the risks from flooding and power failure.

Legislative framework and our guidance

The European & UK Legislative Framework

1.5 The provision of electronic communications networks and services in the UK is regulated under the European Framework on Electronic Communications (the Framework). Originally published in 2002, the Framework comprised five separate Directives[3].

1.6 The European Commission revised the Framework in November 2009. Among other changes, the revisions extended the obligations on Member States, national regulatory authorities and industry in relation to the security of networks and services. These new obligations were introduced as Article 13a and 13b of the Framework Directive[4].

1.7 Member States were required to implement Article 13a and 13b in national law. In the UK, this was done with revision of the Communications Act 2003 (CA2003), principally with the addition of sections 105A to 105D. The relevant sections of CA2003 are included in Annex 3. They came into force on 26 May 2011.

Ofcom's guidance

1.8 We published our original guidance on the security requirements in sections 105A to 105D on 10 May 2011, with a minor revision for clarity following on 3 February 2012. This guidance applied to all providers of Public Electronic Communications Networks (PECN) and Public Electronic Communications Services (PECS).

1.9 We then published a Call for Inputs on 13 December 2013, seeking views on our plans to update the document. A revised version of the guidance was subsequently published on 8 August 2014. The current document explains changes and additions we propose to make to this current, 2014, version of the guidance.

Next Steps

1.10 We consider that as this consultation is about updating guidance, rather than introducing new regulation, and as it addresses a subject with a relatively narrow audience, 6 weeks is a sufficient period to allow for responses. However, this would result in the response period closing during the holiday season. We have therefore decided to keep the consultation period open for 10 weeks, until the 7 September 2017. We will then consider the responses and we expect to publish our views on them alongside a revised version of the guidance in or around 8 weeks after this.

1.11 We would welcome feedback from stakeholders on any of the discussion or proposals in this consultation. There are several areas in which we are particularly

[3] The Framework Directive (2002/21/EC); the Authorisation Directive (2002/20/EC); the Access Directive (2002/19/EC); the Universal Service Directive (2002/22/EC); and the Directive on privacy and electronic communications (2002/58/EC).

[4] Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive) as amended by Directive 2009/140/EC.

keen to hear views and any alternative proposals. We have noted these in the consultation.

1.12 We will continue to keep the guidance under review and consult from time to time about updating it, when we consider this has become sufficiently beneficial.

Section 2

Security & Availability (s105A)

Overview of obligations & existing guidance

2.1 Section 105A states the following:

Requirement to protect security of networks and services

105A.— (1) Network providers and service providers must take technical and organisational measures appropriately to manage risks to the security of public electronic communications networks and public electronic communications services.

(2) Measures under subsection (1) must, in particular, include measures to prevent or minimise the impact of security incidents on end-users.

(3) Measures under subsection (1) taken by a network provider must also include measures to prevent or minimise the impact of security incidents on interconnection of public electronic communications networks.

(4) A network provider must also take all appropriate steps to protect, so far as possible, the availability of the provider's public electronic communications network.

(5) In this section and sections 105B and 105C—

"network provider" means a provider of a public electronic communications network, and

"service provider" means a provider of a public electronic communications service.

2.2 The mains elements of our existing guidance cover the following:

- Overall risk-based approach to security, considering the ENISA Technical Guideline on Security Measures
- Accountability and expertise
- Supply chain and outsourcing
- Network monitoring
- Cyber security
- Protecting end users
- Minimum Security Standard for Interconnection (NICC ND1643)
- Maintaining availability

2.3 We consider that these areas are all still relevant and should remain in the Guidance. However, there are some areas in which additional guidance, or a change in emphasis, seems appropriate. There are also several new areas which we think should be included. The rest of this section sets outs our proposed changes, and seeks views on them.

Cyber security

2.4 The current guidance identifies the importance to the UK of cyber security and the central role of CPs in this. It also sets out several Government cyber security initiatives that are relevant to the security measures that should be considered under section 105A.

2.5 The profile of cyber security incidents, both in the telecoms sector and elsewhere, has continued to grow since the guidance was published. The motivations behind cyber attacks vary from nuisance and petty vandalism, through varying levels of criminality, up to activities attributed to hostile nation states. Telecommunications networks are often involved, sometimes as conduits for the attack, but also sometimes as the targets. The TalkTalk incident in 2015[5], which led to the loss of personal data and a fine from ICO, is the most notable example of the latter. The level of public and Parliamentary interest showed how much impact even a relatively unsophisticated attack can have.

2.6 Government recognises cyber among the most serious threats to the UK, sitting alongside terrorism and international military conflict. It has made it clear in the National Cyber Security Strategy[6] that it considers regulation will have a role to play in ensuring cyber security is appropriately addressed, particularly by companies operating critical national infrastructure.

2.7 As a result of these factors, we have been increasing our focus on cyber as a key threat to telecoms security which needs to be addressed as part of s105A compliance. We expect this trend to continue in the future. We have written to the major CPs about our expectations in relation to cyber security and included the issue in our bilateral discussions. Our published guidance already discusses cyber security, but we propose to update it to better reflect the importance of this threat.

2.8 Under s105A, the Communications Act 2003 requires CPs to take measures to manage risks to security and availability of their PECN and PECS. It does not limit the types of risks that should be considered and it therefore seems clear that measures to manage cyber risks, such as cyber attack, should be included.

2.9 We propose to modify the guidance to stress that we consider appropriate steps to manage cyber security risks to be an essential part of compliance with s105A[7] and that this should be included alongside other considerations such as compliance with data protection obligations. We will continue to reference assessment against Government's "10 Steps to Cyber Security" and Cyber Essentials as important elements of this (although with some proposed changes, as detailed in paragraph 2.15 & 2.16). We also propose to update the text to recognise the creation of the National Cyber Security Centre, NCSC, and to set the expectation that CPs should be aware of, and where appropriate be following, NCSC's guidance on relevant issues. We will explain that when investigating and considering enforcement action, in additional to general considerations such as those in the ENISA Minimum Security

[5] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/

[6] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

[7] We also propose to explain that we consider cyber security incidents to be within the scope of the reporting requirements in s105B – see Section 3 for more details.

Measures[8], we will look to NCSC for guidance on any cyber-specific measures CPs should be taking.

2.10 The effectiveness of the security measures taken by a CP can ultimately best be judged by testing them. We therefore consider that, for a complex area such as cyber security, vulnerability testing will form an important part of the approach taken by a CP. This issue is discussed in more detail in paragraphs 2.22-2.24.

Risk management & governance

2.11 The current Guidance explains our expectation that CPs will take a risk-based approach to complying with their section 105A obligations. It also sets out the need for a CP to have managerial and technical accountability lines for security in place up to Board level.

2.12 We are concerned that security risks may not always receive sufficient attention at the highest levels in some organisations. We propose to explain that when investigating potential breaches of the obligations, we will usually seek evidence of the risk management processes that were used and of specific risk decisions that were taken. We will expect to see that relevant security risks are regularly considered and have appropriate owners at all levels, up to and including the Board. We will also emphasise the need for CPs to have a sufficient level of internal security capability to ensure those considering such risks are appropriately informed.

2.13 We propose to expand further on our positon in relation to the need for CPs to comply with technical security standards, and how this fits with the obligation to appropriately manage risks to security. Managing risks involves understanding them and putting in place measures to address them where appropriate. External certification against security standards can form a powerful mechanism to demonstrate that a CP has processes in place to do this. We discuss some specific standards which we believe have relevance to s105A below. However, we highlight these standards because we feel they address issues which are likely to be relevant in considering compliance with section 105A, and not because we require CPs to obtain certification against them. During an investigation, we may ask a CP to provide evidence of the measures they have taken in relation to particular issues. Certification against security standards may usefully form part of this evidence, but it is not required, and may not be sufficient, to demonstrate compliance.

2.14 Our primary objective in proposing additional guidance in this area is to acknowledge what we see as the risk of creating a “tick box” approach to security management if we rely too heavily on standards certification. On the one hand, CPs may erroneously consider that they have met their obligations under s105A by simply maintaining certification against all the standards we mention in the guidance, and thus not undertaking the necessary management of actual security risks. On the other hand, CPs may expend resources on maintaining certification which may achieve better security outcomes if used in other ways. In either case, too strong a focus on certifications would risk reducing the level of security that might otherwise be achieved.

[8] https://www.enisa.europa.eu/topics/incident-reporting/for-telcos/guidelines/technical-guideline-on-minimum-security-measures

Cyber Essential Plus

2.15 The current guidance strongly encourages CPs to adopt the Cyber Essentials Scheme themselves, and within their supply chain, noting that it covers basic controls to mitigate common internet based threats and is aimed at all organisations. Since the publication of the guidance, Government has continued to encourage CPs to obtain Cyber Essentials Plus, which requires third party inspection, and it is now a requirement for some Government contracts.

2.16 We propose to revise our guidance in this area slightly. We continue to believe that the controls in the standard represent basic cyber security hygiene factors that all CPs should implement where possible. Obtaining third party certification is a powerful way to demonstrate this has been done. However, the complex range of systems in use by some CPs go beyond the IT systems typically in use by the smaller organisations that the Scheme was initially targeted at. Some CPs have told us that this can make obtaining third party certification against the scheme difficult to achieve, and the costs of doing so may become disproportionate. In the event we conduct a relevant investigation into a CP in this position, we will expect it to explain why obtaining Cyber Essential Plus is not proportionate. We will also continue to expect, among other things, to see evidence that the CP has taken the steps required by Cyber Essentials where appropriate.

Minimum Security Standard for Interconnection – NICC ND1643[9]

2.17 In relation to the section 105A(3) obligation to prevent or minimise the impact of security incidents on network interconnection, the current guidance strongly encourages certification against ND1643. It goes on to explain that in the absence of such certification, alternative evidence that the relevant controls are in place would be sought.

2.18 While most larger CPs have maintained certification against ND1643, it has often been raised with us that the standard may be of little practical value in improving security. There are number of reason for this:

- Many of the controls in the standard are concerned with improving the security of equipment in “shared areas” – rooms or buildings which host equipment belonging to multiple CPs in order to allow them to interconnect their networks. Improving security in shared areas reduces the risk that deliberate or accidental actions by one CP, or its agents, could adversely affect any others present. For this to be effective, all CPs involved need to follow the standard. The overall level of security achieved is often said to be only as good as that of the “weakest link”. While the larger CPs, accounting for the vast majority of served customers, are typically certified, there are many smaller CPs which may be present in these areas, and are generally not certified. The continued lack of universal adoption of the standard undermines the effectiveness of the measures taken by those which have adopted it.

- Certification against the standard has not been accredited by a body such as UKAS[10], despite several efforts to initiate this. This means that any company can issue ND1643 certificates, and there are no checks to ensure all companies

[9] This is a standard published by NICC, the UK telecoms sector’s technical forum which develops interoperability standards. It is available from their website - http://www.niccstandards.org.uk/

[10] UK Accreditation Service

doing so are interpreting the standard consistently. This potentially undermines the value of the certificates.

- The standard itself, although revised several times, was originally developed around 10 years ago, and the nature of interconnection, and the risks presented, have changed considerably in that time.
- Even if the standard were to be universally adopted, a sufficiently motivated attacker would likely still be able to succeed in disrupting the networks in shared areas. There are practical, as well as economic, limits on the level of physical protection that can be achieved in shared areas.

2.19 Despite these concerns, which we recognise have some validity, many of the controls in the standard still appear to represent common sense measures to improve the security of interconnections. We note that NICC is currently reviewing the standard. We would encourage this work to continue, and for a new version with a set of controls that form a contemporary “minimum security standard for interconnection” to be established.

2.20 In order to achieve this, NICC should consult with its members and other stakeholders, including NCSC, to ensure the new document is fit for purpose. We are happy to help facilitate this. We would propose that NICC publish the result as a “best practice” document, rather than a standard against which CPs would be certified. We would then continue to use the document, in its revised form, as a reference point when determining if a CP has taken appropriate measures to comply with 105A(3).

2.21 We also propose to note that, whatever the status of ND1643, the obligation on CPs to take measures to prevent or minimise the impact of security incidents on network interconnections remains. In that regard, we note that, as required by Article 13a(1) of the Framework Directive, the measures to be taken by CPs must ensure a level of security appropriate to the risk presented “*having regard to the state of the art*” and therefore we would ourselves have regard to the state of the art of such measures in any compliance assessment.

Cyber vulnerability testing

2.22 For several years, the Bank of England has been operating a cyber vulnerability testing framework[11] to assess the level of cyber security in place in key financial organisations. DCMS is leading a project involving Ofcom, NCSC and industry to develop a similar scheme for the telecoms sector. The intention is that detailed intelligence on the threats faced by the CP undergoing testing would be gathered, and would form the basis for various penetration tests undertaken on their operational networks. As well as assessing how well defended the CP’s network is against such attacks, such testing would also show how well it could detect and respond to any successful attempts.

2.23 We believe such a scheme has great potential to increase both the level of cyber security that CPs have in place, and the level of assurance among ourselves and Government of CPs’ ability to defend against and respond to real world attacks. We also consider that this approach would be more effective than reliance on security standard certification alone.

[11] http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx

2.24 We propose to explain that we will be looking to CPs to participate in this scheme when the DCMS led pilot phase is complete and the scheme is adapted for the Telecoms sector.

Maintaining network availability

2.25 The current guidance says that CPs should take measures to maintain availability which are appropriate to the needs of their direct customers. An exception to this general obligation is for networks providing access to the emergency organisations, in relation to which CPs should also ensure they comply with the specific availability requirements in the relevant General Condition[12].

2.26 We consider that the existing advice remains generally appropriate. However, there are a number specific areas, beyond the existing mention of access to the emergency organisations, in which we feel additional guidance on our expectations in relation to availability may be helpful.

2.27 As the reliance on communications services continues to grow, so do the expectations placed upon them, and the networks supporting them. Increasing amounts of work to improve and monitor network coverage and quality of service, and the introduction of automatic compensation for customers who suffer from loss of service, are examples of this. We believe these increased expectations apply to network availability too, on both fixed and mobile networks.

2.28 CPs are required by 105A(4) to “take all appropriate steps to protect, so far as possible, the availability” of their networks. If we need to consider whether a CP has taken “all appropriate steps”, there are several issues we will consider in particular. We propose to amend the guidance as set out below to reflect this.

Single points of failure

2.29 By single points of failure, we mean instances in which the network relies on significant amounts of traffic passing over a single route, a single point of handover, or on routing through a single location, thereby leaving the service vulnerable to a single point of failure.

2.30 We propose to explain that we consider that avoiding single points of failure, where it is reasonably possible to do so, is likely to be an “appropriate step” within the meaning of s105A(4). We will note that the extent to which avoiding single points of failure is reasonably possible will vary at different points in the network, and will give some examples of relevant considerations, including:

- it is more likely to be disproportionate to deploy protection paths in the access network than in a CP’s backhaul and core networks;
- the number of customers relying on the single point of failure; and
- other issues such as geographic and physical constraints.

[12] We are currently in the process of reviewing these General Conditions of Entitlement. We propose to update the reference in the Guidance to reflect any changes in content and numbering of the relevant Condition.

2.31 We have seen a number of reported incidents in which damage to transmission route optical fibres at a single location, or the disruption of a single building, has caused the loss of connectivity to large numbers of access nodes and hence large numbers of customers. Such situations are of particular concern when they result in loss of service to a significant geographical area, potentially isolating whole communities[13]. When investigating such incidents, we will seek evidence that the CP has assessed the risks involved in their network design choices, and has met their obligations to take all appropriate steps to protect availability.

Flood resilience

2.32 Several of the larger network owning CPs took part in the National Flood Resilience Review recently completed by the Cabinet Office. This involved those companies using the latest flood prediction data to assess the vulnerable of key sites in their networks and considering the need for defences where required. This resulted in CPs investing in additional temporary and permanent flood defences. In light of the increase frequency and severity of flood events, we welcome this activity and consider it to be in line with the requirements imposed by 105A(4).

2.33 We propose to update the guidance to reflect the growing risk to availability from flooding and our expectation that CPs continue to take steps to manage it appropriately. We will note that, even where sites are identified as being at a lower risk of flooding, CPs should still consider whether additional measures are required for other reasons, for example because they represent a potential single point of failure for a significant number of customers. We will also explain that we expect to more closely examine the mitigation steps taken by CPs following significant flood incidents, and will launch formal investigations if appropriate.

Power resilience

2.34 A loss of mains power is cited as the root cause in many of the incident reports that we receive. Even for incidents linked to severe weather or flooding, it is often the associated loss of power that is the actual cause of the communications outages. CPs typically explain that key nodes in the core of their networks have sufficient backup power to continue functioning for several days or more. Moving towards the access nodes, the level of resilience will typically reduce, for both practical and economic reasons.

2.35 We expect CPs to manage the risks of power failure to their network availability appropriately and propose to reflect an increased focus on this issue in our revised guidance. As with flooding, we propose to indicate that we expect to closely examine, and where appropriate investigate, significant availability incidents involving power loss. In parallel with this consultation, we are planning to seek information from some CPs on their current network power resilience provision with a view to publishing an overview analysis in our Connected Nations report.

Outsourcing

2.36 Many CPs make extensive use of third parties to provide infrastructure for, and to design and operate, their networks. In these cases, the CP may have less visibility or

[13] This may be a particular concern if the community is geographically remote and a combination of logistical challenges, including adverse weather preventing physical access or supply chain operation, could lead to an extended service outage.

control over the level of resilience that is put in place than it would if it kept these activities in-house.

2.37 We propose to explain in the revised Guidance that we do not consider that outsourcing to third parties in this way excuses CPs from their obligations under 105A(4). Put simply, a CP cannot contract out of its statutory obligations. As such, they need to have sufficient levels of contractual control over third parties in place to ensure they continue to comply with their obligations. Furthermore, we expect CPs to check, on an ongoing basis, that actions undertaken on their behalf do not put them in breach of their obligations.

Section 3

Incident Reporting (s105B)

Overview of obligations & existing guidance

3.1 Section 105B states the following:

Requirement to notify OFCOM of security breach

105B – (1) A network provider must notify OFCOM –

(a) of a breach of security which has a significant impact on the operation of a public electronic communications network, and –

(b) of a reduction in the availability of a public electronic communications network which has a significant impact on the network.

(2) A service provider must notify OFCOM of a breach of security which has a significant impact on the operation of a public electronic communications service.

(3) If OFCOM receive a notification under this section, they must, where they think it appropriate, notify—

(a) the regulatory authorities in other member States, and

(b) the European Network and Information Security Agency ("ENISA").

(4) OFCOM may also inform the public of a notification under this section, or require the network provider or service provider to inform the public, if OFCOM think that it is in the public interest to do so.

(5) OFCOM must prepare an annual report summarising all notifications received by them under this section, and any action taken in response to a notification.

(6) A copy of the annual report must be sent to the European Commission and to ENISA.

3.2 Our current Guidance covers the following:

- How and when to report
- Qualitative and quantitative thresholds
- Format and content of reports
- Incident follow-up
- Annual reporting summary

3.3 For the most part, we consider that reporting is working well and the structure of the current guidance remains appropriate. However, there are several areas in which we propose making changes which are described in the remainder of this section.

3.4 Since the guidance was last revised, we have written to the CPs which report most often to set out our expectations in relation to the reporting of cyber security and urgent incidents. We propose to update the guidance to reflect this, taking into account what we have learnt since establishing these new procedures, and using this as an opportunity to simplify things slightly.

3.5 We are concerned that the current thresholds for reporting of incidents affecting mobile services is resulting in significant differences between the mobile network operators in deciding which incidents should be reported and how their impacts should be calculated. We therefore propose to adopt new mobile reporting thresholds and more prescriptive guidance on how customer impact is calculated.

3.6 We also propose making a minor amendment to the current explanation of the incident follow up process.

Mobile reporting

3.7 When we last reviewed our guidance, and in subsequent discussions with mobile operators, we have explained that the fact we consistently receive a much lower number of incidents reports in relation to mobile services than we do for fixed is of concern. Mobile services are now as important, or more important, to many customers than fixed services, and so we need to know what has happened when they go wrong.

3.8 Reporting is important for several reasons. It allows us to know about, and if necessary investigate and take enforcement action in relation to, specific incidents where a CP may have fallen short of its security or resilience obligations. The clear majority of reported incidents do not fall into this category however. Instead they are examples of more routine problems which inevitably occur when running complex networks in the real world. Reporting of such incidents is still relevant, because it allows us to determine why they occurred and how the CP has handled them, and therefore whether the security measures it has in place are appropriate. When we don’t receive any incident reports from a mobile operator for an extended period, not only does this raise concerns that its reporting process may be inadequate, it also reduces our ability to judge its compliance with s105A.

3.9 As previously acknowledged in our guidance, there are a number of practical reasons why reporting for mobile networks is more complex than fixed, and why the number and nature of the incidents is likely to be different. At the time of our last guidance review, we therefore decided to set reporting thresholds individually with each of the four main mobile network operators. This approach was intended to arrive at similar reporting thresholds for each operator, but in a way which reflected how they each detected and responded to major incidents, hence minimising any unnecessary reporting burden.

3.10 Following publication of our current guidance, this approach initially led to more frequent and consistent reporting from all operators, but over time this has changed. Some operators have responded to our requests for more regular reporting with new approaches which greatly increase the volume of incident reports we receive. Others, in contrast, are reporting far less frequently than they originally did under the current arrangements. It also appears that there are a wide variety of approaches used by operators for calculating the level of customer impact of an incident. We do not believe the resulting discrepancy in the number and scale of reported incidents is attributable to differences in the underlying resilience of the operators’ networks. We consider that we should revise our mobile reporting guidance and thresholds to address these inconsistencies.

Mobile reporting thresholds

3.11 Establishing numerical reporting thresholds for mobile networks is more complex than for fixed networks. Generally, when elements of a fixed network fail, it is reasonably straightforward to determine how many customers were connected to them and hence lost service and therefore whether the incident is reportable.

3.12 Because there is not a static relationship between individual customers and particular elements of the mobile network, the same approach cannot be used. Methods for establishing customer impact typically rely on estimating of how many customers may have been trying to use the affected parts of the network based on historical data. Some mobile operators have previously told us that they consider it to be unduly burdensome to produce such estimates for every incident that occurs simply in order to see if they meet a numerical reporting threshold, when the vast majority will not.

3.13 The approach we adopted of allowing mobile operators to report incidents which triggered their own major incident management processes was intended to remove the need to undertake these potentially complex customer impact estimates for each incident to determine whether it should be reported. Each mobile operator has multiple criteria for determining the severity of incidents and these vary by operator. Generally, the criteria include an assessment of the scale of impact on the network infrastructure, such as the number of sites affected.

3.14 To ensure a more consistent basis for reporting we propose to set aside the previously agreed reporting triggers, and in their place set specific numerical thresholds applicable to all mobile network operators. Given the difficulties of estimating customer impact discussed above, we propose to base these thresholds on the impact to network infrastructure.

3.15 We set out our proposed new thresholds below, and this is an area on which we are particularly keen to hear views and any alternative suggestions from stakeholders. Our objective is to receive a significant and sustained increase in reporting from those MNOs which are currently reported infrequently, while avoiding a reporting process which is unduly burdensome.

3.16 We also need to ensure that we hear about all incidents which have a significant impact. We consider that this will imply different types of incident depending on how dense or sparsely populated the affected area is. In the event of incidents affecting service from specific sites:

- in urban areas, it is more likely that the MNO will have coverage from other sites which overlaps or is near the affected area. It is also more likely that other MNOs will have unaffected coverage, allowing for roamed emergency calls to be made. Therefore, for the impact of the incident to be significant, it is likely to have to affect a relatively large number of sites;

- In rural areas, it is more likely that the loss of service from even a single site could completely isolate a community from all mobile coverage, including the ability to make emergency calls. Travelling to find service elsewhere is also likely to be more onerous or impractical. Therefore, the impact of an incident may still be significant if it affects only a small number of sites, or even a single site, for an extended period.

3.17 Some incidents causing a significant impact are not linked to specific sites at all, and we need to ensure our guidance leads to these also being reported. We consider that our existing qualitative criteria will capture any such incidents which are not otherwise caught by the numerical criteria below.

3.18 Our proposals for numerical reporting criteria for mobile are as follows:

Network/service type	***Minimum extent of service loss or major disruption***[2]	***Minimum duration of service loss or major disruption***
Mobile voice or data service/network offered to retail customers	*Service loss or major disruption to voice and/or data services for one or more technology (i.e. 2G, 3G and/or 4G) from 25 or more sites*	*2 hours*
Mobile voice or data service/network offered to retail customers in rural areas[1]	*Service loss or major disruption for all voice and/or all data services from 1 or more sites*	*8 hours*

Note on table:

[1] For these purposes, the incident should be considered to affect a rural area if any of the sites affected by an incident is located in a rural area, according to a recognised rural/urban classification. Ofcom typically uses the Locale classification[14] as the basis for our own geographic analysis. Government also publishes a suitable classification available from https://www.gov.uk/government/collections/rural-urban-classification.

[2]Incidents meeting these criteria should be reported, regardless of whether emergency roaming may have been available.

Calculating the number of users affected

3.19 The current guidance asks CPs to provide an estimate of the number of users, sometimes referred to as end customers, affected by reported incidents. Although accurate estimates of customer numbers can be difficult to produce for mobile incidents, we propose to continue to require operators to provide such estimates. These estimates are important to allow us to quickly understand the relative impact of different incidents. Another reason is that we are required to provide an annual summary of all incidents resulting in more than one million customer hours of service loss to the European Commission.

3.20 We propose to modify paragraph 4.29 of the current guidance to remove the brackets, as follows:

[14] http://www.bluewavegeographics.com/images/LOCALE_Classification.pdf

> *Where exact numbers are not available we expect the CP to use historical data to estimate the number of end customers affected.*

3.21 We further propose to add a new paragraph following this, which will explain how to calculate the number of users affected by a mobile outage, as follows:

> *For incidents affecting mobile networks, the CP should calculate the number of customers affected using recent historical network records from the same day(s) of the week and times of the day as the incident, as follows:*
>
> - *First establish the total number of customers typically connecting to the network via each affected mobile site and technologies during each one-hour period covered by the incident. Where an incident lasts for more than 24 hours, the totals should only be calculated for the first 24 one-hour periods covered by the incident.*
> - *For each site, the number of customers affected should be calculated as the average of the site's hourly totals calculated above.*
> - *The total number of customers affected by the incident should be calculated as the sum of these averages across all affected sites.*

3.22 This approach will yield a customer impact figure which is essentially the average number of customers normally attached to the network via the affected sites, during any one-hour period. It does not allow for the possibility that some affected customers were able to attach to the network via unaffected sites, and could therefore be considered to risk over-estimating the impact. However, as it is likely that different customers would move into the affected area during the course an incident, using the average of the hourly totals is likely to lead to an under-estimate. We consider that the proposed approach strikes a reasonable balance between an acceptably accurate estimate, and the need to undertake much more complex calculations.

3.23 We note that, for some CPs, this calculation may nonetheless be more onerous than those used in their current customer impact estimates. However, we reiterate that our objective is to ensure all CPs offering mobile services are calculating estimates in a comparable fashion. We consider that the burden is not likely to be excessive, as the calculations are only required in relation to incidents which have already been found by the CP to meet the reporting criteria.

3.24 The current guidance explains that information on the number of users affected should be as accurate as technically feasible at the time of reporting. We propose to expand on this point by noting that for mobile incidents, the detailed estimates explained here are unlikely to be available for some time after the incident has been resolved. We will ask CPs to update any initial incident reports with this information when it is reasonably available.

3.25 We note the potential links between mobile reporting under s105B and the work we are doing elsewhere on customer experience issues. In particular, in our recent consultation on automatic compensation[15], we explained that we would be undertaking further work to monitor the degree of mobile service loss customers are experiencing.

[15] https://www.ofcom.org.uk/consultations-and-statements/category-1/automatic-compensation

Reporting affected sites

3.26 Some CPs provide a full list of affected sites in relation to reported mobile incidents. We have found this very useful in developing an understanding of the geographic extent of an incident.

3.27 We propose to add an additional paragraph after paragraph 4.32 in the current guidance, as follows:

> *Where an incident has affected mobile base station sites, the CP should include a list of all affected sites and their location in its incident report.*

Cyber incident reporting

3.28 As with the obligations to include cyber risks when considering security measures as discussed in Section 2, we consider that cyber security incidents are within the scope of the notification obligations in s105B. We have already noted this in our communications with CPs. In December 2015 we wrote to the CPs that regularly report incidents to set out a new process and thresholds for the reporting of urgent incidents (see paragraph 3.36). These thresholds included two for major cyber security incidents.

3.29 We propose to update our guidance to ensure all CPs are aware that cyber incidents are reportable, and what the thresholds for doing so are. Section 105B requires incidents which have a “significant impact on the operation” of a network or service to be reported. Our current guidance gives indicative thresholds for the duration and scale of service outage for an incident to be considered significant and therefore reportable. However, not all significant incidents result in high levels of service outage, or indeed any service outage at all.

3.30 Experience from the examples we have seen to date suggests this is often the case for cyber incidents. Very few cyber incidents that have been reported, or that we have become otherwise aware of, have resulted in service outage. More typically, they involve major breaches of data confidentiality or integrity, both of which we consider can constitute a significant impact on the operation of a service.

3.31 Alongside the numerical reporting thresholds, the existing guidance has a number of qualitative criteria. These are intended to identify incidents which may not have resulted in major service outage, but have other features which suggest their impact may be significant and they should therefore be reported. We consider that most major cyber incidents will trigger one or more of these criteria.

3.32 We feel that it is particularly important that we are aware of all incidents that could be considered to have a “significant impact” in order that we can assess and if necessary investigate them further. However, we are concerned that for some CPs, cyber incidents may be dealt with separately to the types of incident more typically reported under s105B. For the avoidance of doubt on this point, we propose adding an additional qualitative criterion to the list of reportable incidents as follows:

- *Any incidents involving cyber security breaches, which meet any of the criteria in this paragraph.*

3.33 We acknowledge that there may be more subjective judgement involved in assessing whether an incident should be reported under this criterion than others in the current guidance. The number of cyber incidents we have dealt with is still small and they tend to be quite different both in their makeup and impact. This makes setting simple criteria which unambiguously identify those incidents which have a significant impact, and should therefore be reported, difficult.

3.34 We would welcome input from stakeholders on this issue and whether further guidance on this criterion would be beneficial. We stress here that we would always rather CPs over, rather than under, report, so if there is any doubt about an incident we would encourage CPs to report it. While we intend the guidance to be of assistance wherever possible, like all other areas of reporting, the obligation on CPs to identify and report incidents which have a “significant impact” will ultimately require them to use their own judgement.

3.35 We acknowledge the broader national security concerns raised by some cyber incidents. We propose to note in the guidance that we will ensure information is dealt with by individuals with the appropriate level of security clearance where this is required, in agreement with Government agencies.

24/7 reporting process for urgent incidents and subsequent changes to other reporting timescales

3.36 Security incidents in the telecoms sector which have been serious enough to generate large amounts of political or media interest have thankfully been rare. However, they do occasionally occur, and some have occurred outside normal business hours. While the current process is generally working well, in some cases Ofcom has received enquiries or seen media reports about very serious incidents before we have been notified by the CP involved. Examples include cyber security incidents with little or no impact on service availability, and incidents which take place in the evening, during the weekend or during bank holidays.

3.37 Ofcom does not wish to unduly intrude on live incident management processes, but it is important that we are aware of such incidents and can assure ourselves that they are being dealt with by the CP concerned.

3.38 We wrote to the operators which regularly report incidents to us in December 2015. In this letter, we set out a change to reporting process published in our guidance which was intended to ensure that basic information about certain urgent incidents are reported to us as quickly as possible, via 24/7 telephone and e-mail reporting arrangements. We propose to update the published guidance to reflect an updated version of this urgent incident reporting process.

Proposed changes to the current incident “categories”

3.39 The published incident reporting process allows for three different reporting deadlines, depending on the significance of the incident. Where a CP has several smaller, routine incidents, these can be reported in batches, at least once per month, which is the approach adopted by most CPs. For major incidents or incidents that are likely to generate media or political interest, the guidance states an expectation that incidents are reported within 24 hours. All other incidents should “ideally be reported within a few days of the incident commencing”.

3.40 Although we propose introducing the new category of “urgent” incidents with shorter reporting timescales into the guidance, we are keen to keep the process as simple as possible. We therefore propose reverting to three separate incident categories in the revised guidance from the four currently in place (the three set out in the existing guidance and the “urgent” category introduced in our December 2015 letter). To achieve this, we propose replacing paragraphs 4.5-4.7 in existing guidance as follows:

> *Urgent incidents should be reported, whenever possible, within 3 hours of the CP becoming aware. The criteria for identifying Urgent incidents, and the reporting process, is set out below.*
>
> *Other incidents should be reported, whenever possible, within 72 hours of the CP becoming aware.*
>
> *Where a CP has a significant number of 'non major' incidents (typically those meeting only the lowest fixed numerical threshold), these may be reported in batches.*
>
> *All batched incidents which commenced in a calendar month must be reported to Ofcom before the second Monday of the following month.*

3.41 We propose the deadline of 72 hours to align with the notification requirements in the General Data Protection Regime (GDPR). This would replace the current deadline, and although more specific than the current wording (which says "within a few days") we don't consider that this should require a material change to most CPs' current processes. We consider that, given we are proposing that the most urgent incidents are notified to us much more quickly (within 3 hours), it is appropriate for other incidents to be reported to this longer timeframe.

3.42 We propose noting that we do not expect a CP will always have full and accurate details of an incident and its impact within the reporting timescales. It is therefore acceptable for the CP to provide updated reports beyond the deadline with updated and/or additional information as it becomes available. In the case of urgent incident reports we appreciate that the information available for the initial report may be very limited and may consist of no more than informing us that the CPs is aware of an incident and is investigating.

3.43 We are not proposing any changes to the arrangements to reporting batched incidents. However, we propose adding an additional note to stress the importance of CPs having adequate processes in place to ensure this reporting is done routinely. We have seen several examples where CPs' reliance on specific individuals who have changed employer or role, or otherwise been unavailable, has resulted in a lack of regular reporting.

Urgent incident criteria

3.44 We propose adding a new set of criteria to the guidance which will help CPs identify incidents which should be reported under the urgent reporting process. These criteria are not intended to capture any incidents that would not otherwise be reportable under the general qualitative criteria and numerical thresholds. Instead, they are intended to identify a subset of those reportable incidents which we believe should be reported to us more quickly than usual.

3.45 The proposed urgent reporting criteria are:

- *Cyber-attacks meeting any of the qualitative criteria for reportable incidents in paragraph x.xx*
- *Incidents affecting services to 10M end users*

- *Incidents affecting services to 250k end users and expected to last 12 hours or more*
- *Incidents attracting national mainstream media coverage*
- *Incidents affecting critical Government or Public Sector services (e.g. wide spread impact on 999, 3-digit non-emergency numbers, emergency services communications)*

Urgent incident reporting process

3.46 We propose to explain the process for reporting urgent incidents by replacing Figure 2 in the existing guidance with the revised Figure 2 below, and inserting the following text:

> *Where an incident meets one of the above urgent reporting criteria, the communications provider should contact Ofcom via the agreed contacts, or the 24/7 reporting number*[16] *where they are unavailable, as soon as possible. Under all but the most exceptional circumstances, we expect this initial contact to have been made within 3 hours.*

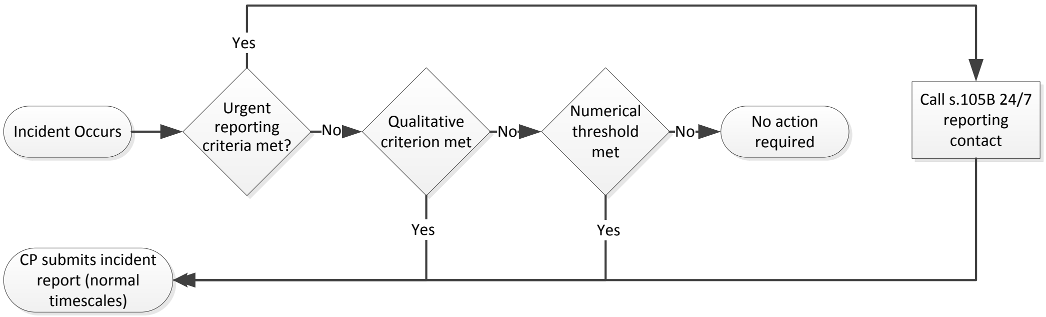
Incident Occurs
Urgent reporting criteria met?
Yes
No
Qualitative criterion met
No
Yes
Numerical threshold met
No
Yes
No action required
Call s.105B 24/7 reporting contact
CP submits incident report (normal timescales)

Figure 2 – Proposed new "Incident Reporting Process" diagram

Incident follow up

3.47 The current guidance includes as Figure 3 a diagram of the incident follow up process. We propose to replace this diagram with the modified version shown below (Figure 3). This is identical to the process shown in the current guidance, but with the latter stages removed. We consider that these latter elements went beyond the incident follow up process itself, and towards enforcement. As discussed in Section 4, our enforcement approach will be in line with our separately published Enforcement Guidelines, and hence we do not wish to create confusion or potential conflict by including overlapping elements here.

[16] This number will be shared directly with CPs which Ofcom considers may need to report urgent incidents. We do not propose including it in the published guidance.

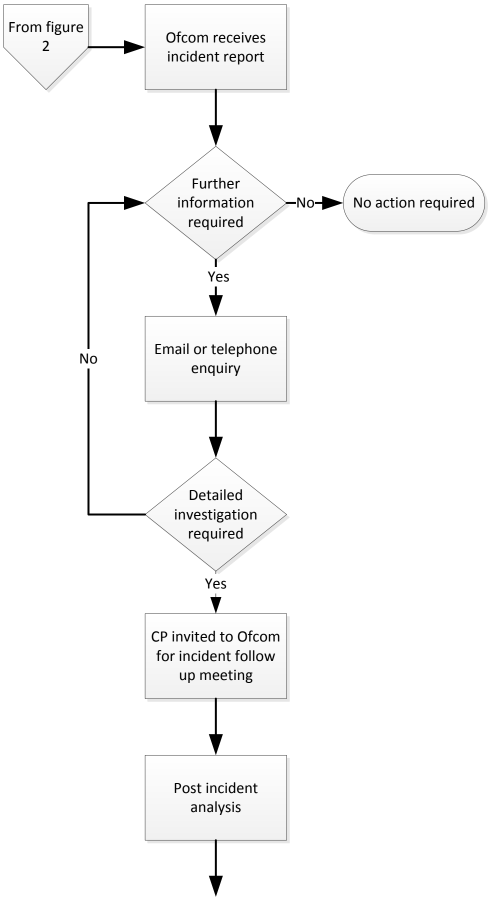
From figure 2
Ofcom receives incident report
Further information required
No
No action required
Yes
Email or telephone enquiry
No
Detailed investigation required
Yes
CP invited to Ofcom for incident follow up meeting
Post incident analysis

Figure 3 – Proposed new "Incident Follow up Process" diagram

Section 4

Audit & Enforcement (s105C & D)

4.1 The current guidance briefly sets outs our relevant powers to undertake audits, take enforcement action, and gather information. It then sets out some examples of situations which might trigger the use of these powers.

4.2 We propose to replace this section of the guidance with two separate sections covering auditing and enforcement. The rest of this section explains what we propose to include in each of them.

Auditing

4.3 Section 105C places a requirement on CPs to co-operate with, and pay the cost of, any audits undertaken by Ofcom, or on our behalf, of the measures taken by it under s105A.

4.4 In the current version of the guidance, we explain that we may consider the need for an audit where we have asked a provider for evidence of compliance with sections 105A or 105B and they have not provided an acceptable response. We also explain that we only expect to exercise our ability to audit as a backstop measure in exceptional cases.

Frequency of s105C audits

4.5 We have discussed earlier in this consultation that concerns about the potential effect on the UK from telecoms security failings, for example caused by flooding or cyber attack, have increased since our current guidance was published. This has resulted in calls for assurance that the security measures taken by CPs are adequate to ensure major incidents cannot occur.

4.6 Such assurance can never be 100%. Even with state of the art security measures in place, we recognise that security incidents can and will still occur. However, we consider that increasing the use of the auditing powers in s105C may have a role in improving confidence that CPs are taking appropriate security measures under s105A. Auditing is not the only tool that will contribute to this. Our information gathering powers are relevant, as is our ongoing direct engagement with individual CPs. Other proposals in this consultation, such as the adoption of cyber vulnerability testing and an increased focus on investigating resilience failures, will also have a role.

4.7 We propose to change the current guidance to reflect that we may consider exercising the power to conduct audits more often than previously.

4.8 We are aware of that audits are potentially a significant burden on CPs. This is due both to the direct cost on them of paying for the auditing work, but also the internal resources required to support it. We propose to note that we will consider the appropriateness of auditing carefully in each case, albeit potentially more often than we have to date.

Purpose of an audit

4.9 The use of our auditing powers will be specific to the situation we are considering and therefore likely to be different in each case. In general, our objective will be to find evidence of the measures that a CP has taken to manage a particular risk, in order to inform an assessment of whether it has complied with s105A. The relevant standards and best practice we refer to in the guidance will usually form the basis for an audit where these are relevant to the area of concern.

4.10 To give an example, in which we are considering whether a CP, or group of CPs, had appropriate risk management measures in place, we would be likely to include an assessment of the security objective "SO2: Governance and Risk Management" from the ENISA Technical Guideline[17] in any audit. As such, the auditor might be seeking, among other things, evidence that the CP had a documented risk management methodology which is in line with industry standards, and that it was followed.

4.11 As another example, we might use an audit to seek evidence that a specific technical measure had been undertaken. For example, if we would have concerns about the measures taken to protect a CP's internet connected desktop PCs, we might focus an audit on whether security patches had been applied within 14 days of becoming available, in line with a control in the Cyber Essentials Scheme.

Enforcement

4.12 Ofcom publishes Enforcement Guidelines, which set out how we investigate compliance with, and approach enforcement of, regulatory requirements across a range of areas. In January of this year, we consulted[18] on changes to these Enforcement Guidelines, and have recently published our statement and revised procedures[19].

4.13 The revised Enforcement Guidelines[20] notes that the procedures it sets out cover any action we take in relation to s105A-C compliance. We therefore do not intend to include any additional detail in relation to our enforcement approach in our revised security guidance, and will instead simply refer CPs to the Enforcement Guidelines for more information.

4.14 We propose to note that in relation to specific incidents, it will often be more effective for us to work informally with stakeholders, given that the priority will usually be to learn from incidents and avoid repeats. However, we will not be slow to use our formal enforcement powers where we consider that to be appropriate.

[17] https://www.enisa.europa.eu/publications/technical-guideline-on-minimum-security-measures/at_download/fullReport

[18] https://www.ofcom.org.uk/consultations-and-statements/category-2/ofcoms-approach-to-enforcement

[19] https://www.ofcom.org.uk/consultations-and-statements/category-2/ofcoms-approach-to-enforcement?utm_source=updates&utm_medium=email&utm_campaign=approach-enforcement

[20] https://www.ofcom.org.uk/__data/assets/pdf_file/0015/102516/Enforcement-guidelines-for-regulatory-investigations.pdf

Annex 1

Responding to this consultation

How to respond

A1.1 Ofcom would like to receive views and comments on the issues raised in this document, **by 5pm on 7 September 2017**.

A1.2 We strongly prefer to receive responses via the online form at https://www.ofcom.org.uk/consultations-and-statements/category-1/review-security-guidance. We also provide a cover sheet (https://www.ofcom.org.uk/consultations-and-statements/consultation-response-coversheet) for responses sent by email or post; please fill this in, as it helps us to maintain your confidentiality, and speeds up our work. You do not need to do this if you respond using the online form.

A1.3 If your response is a large file, or has supporting charts, tables or other data, please email it to SecurityConsultation@ofcom.org.uk, as an attachment in Microsoft Word format, together with the cover sheet (https://www.ofcom.org.uk/consultations-and-statements/consultation-response-coversheet). This email address is for this consultation only, and will not be valid after 7 September 2017.

A1.4 Responses may alternatively be posted to the address below, marked with the title of the consultation.

Ben Willis
Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA

A1.5 If you would like to submit your response in an alternative format (e.g. a video or audio file), please contact Ben Willis on 020 7783 4681, or email ben.willis@ofcom.org.uk

A1.6 We do not need a paper copy of your response as well as an electronic version. We will acknowledge receipt if your response is submitted via the online web form, but not otherwise.

A1.7 You do not have to answer all the questions in the consultation if you do not have a view; a short response on just one point is fine. We also welcome joint responses.

A1.8 It would be helpful if you could explain why you hold your views, and what you think the effect of Ofcom's proposals would be.

A1.9 If you want to discuss the issues and questions raised in this consultation, please contact Ben Willis on 020 7783 4681, or by email to ben.willis@ofcom.org.uk

Confidentiality

A1.10 Consultations are more effective if we publish the responses before the consultation period closes. In particular, this can help people and organisations with limited resources or familiarity with the issues to respond in a more informed way. So, in the interests of transparency and good regulatory practice, and because we believe it is important that everyone who is interested in an issue can see other respondents' views, we usually publish all responses on our website, www.ofcom.org.uk, as soon as we receive them.

A1.11 If you think your response should be kept confidential, please specify which part(s) this applies to, and explain why. Please send any confidential sections as a separate annex. If you want your name, address, other contact details or job title to remain confidential, please provide them only in the cover sheet, so that we don't have to edit your response.

A1.12 If someone asks us to keep part or all of a response confidential, we will treat this request seriously and try to respect it. But sometimes we will need to publish all responses, including those that are marked as confidential, in order to meet legal obligations.

A1.13 Please also note that copyright and all other intellectual property in responses will be assumed to be licensed to Ofcom to use. Ofcom's intellectual property rights are explained further at http://www.ofcom.org.uk/terms-of-use/

Next steps

A1.14 Following this consultation period, Ofcom plans to publish a statement in or around November 2017.

A1.15 If you wish, you can register to receive mail updates alerting you to new Ofcom publications; for more details please see http://www.ofcom.org.uk/email-updates/

Ofcom's consultation processes

A1.16 Ofcom aims to make responding to a consultation as easy as possible. For more information, please see our consultation principles in Annex 2.

A1.17 If you have any comments or suggestions on how we manage our consultations, please call our consultation helpdesk on 020 7981 3003 or email us at consult@ofcom.org.uk. We particularly welcome ideas on how Ofcom could more effectively seek the views of groups or individuals, such as small businesses and residential consumers, who are less likely to give their opinions through a formal consultation.

If you would like to discuss these issues, or Ofcom's consultation processes more generally, please contact Steve Gettings, Ofcom's consultation champion:

Steve Gettings
Ofcom
Riverside House
2a Southwark Bridge Road
London SE1 9HA

Tel: 020 7981 3601
Email steve.gettings@ofcom.org.uk

Annex 2

Ofcom’s consultation principles

Ofcom has seven principles that it follows for every public written consultation:

Before the consultation

A2.1 Wherever possible, we will hold informal talks with people and organisations before announcing a big consultation, to find out whether we are thinking along the right lines. If we do not have enough time to do this, we will hold an open meeting to explain our proposals, shortly after announcing the consultation.

During the consultation

A2.2 We will be clear about whom we are consulting, why, on what questions and for how long.

A2.3 We will make the consultation document as short and simple as possible, with a summary of no more than two pages. We will try to make it as easy as possible for people to give us a written response. If the consultation is complicated, we may provide a short Plain English / Cymraeg Clir guide, to help smaller organisations or individuals who would not otherwise be able to spare the time to share their views.

A2.4 We will consult for up to ten weeks, depending on the potential impact of our proposals.

A2.5 A person within Ofcom will be in charge of making sure we follow our own guidelines and aim to reach the largest possible number of people and organisations who may be interested in the outcome of our decisions. Ofcom’s Consultation Champion is the main person to contact if you have views on the way we run our consultations.

A2.6 If we are not able to follow any of these seven principles, we will explain why.

After the consultation

A2.7 We think it is important that everyone who is interested in an issue can see other people’s views, so we usually publish all the responses on our website as soon as we receive them. After the consultation we will make our decisions and publish a statement explaining what we are going to do, and why, showing how respondents’ views helped to shape these decisions.

Cover sheet for response to an Ofcom consultation

BASIC DETAILS

Consultation title:

To (Ofcom contact):

Name of respondent:

Representing (self or organisation/s):

Address (if not received by email):

CONFIDENTIALITY

Please tick below what part of your response you consider is confidential, giving your reasons why

Nothing	□	Name/contact details/job title	□
Whole response	□	Organisation	□
Part of the response	□	If there is no separate annex, which parts?	

If you want part of your response, your name or your organisation not to be published, can Ofcom still publish a reference to the contents of your response (including, for any confidential parts, a general summary that does not disclose the specific information or enable you to be identified)?

DECLARATION

I confirm that the correspondence supplied with this cover sheet is a formal consultation response that Ofcom can publish. However, in supplying this response, I understand that Ofcom may need to publish all responses, including those which are marked as confidential, in order to meet legal obligations. If I have sent my response by email, Ofcom can disregard any standard e-mail text about not disclosing email contents and attachments.

Ofcom seeks to publish responses on receipt. If your response is
non-confidential (in whole or in part), and you would prefer us to
publish your response only once the consultation has ended, please tick here.

Name Signed (if hard copy)

Annex 3

Communications Act 2003 wording

Security of public electronic communications networks and services

Requirement to protect security of networks and services

105A.—(1) Network providers and service providers must take technical and organisational measures appropriately to manage risks to the security of public electronic communications networks and public electronic communications services.

(2) Measures under subsection (1) must, in particular, include measures to prevent or minimise the impact of security incidents on end-users.

(3) Measures under subsection (1) taken by a network provider must also include measures to prevent or minimise the impact of security incidents on interconnection of public electronic communications networks.

(4) A network provider must also take all appropriate steps to protect, so far as possible, the availability of the provider's public electronic communications network.

(5) In this section and sections 105B and 105C—

"network provider" means a provider of a public electronic communications network, and

"service provider" means a provider of a public electronic communications service.

Requirement to notify OFCOM of security breach

105B.—(1) A network provider must notify OFCOM—

(a) of a breach of security which has a significant impact on the operation of a public electronic communications network, and'

(b) of a reduction in the availability of a public electronic communications network which has a significant impact on the network.

(2) A service provider must notify OFCOM of a breach of security which has a significant impact on the operation of a public electronic communications service.

(3) If OFCOM receive a notification under this section, they must, where they think it appropriate, notify—

(a) the regulatory authorities in other member States, and

(b) the European Network and Information Security Agency ("ENISA").

(4) OFCOM may also inform the public of a notification under this section, or require the network provider or service provider to inform the public, if OFCOM think that it is in the public interest to do so.

(5) OFCOM must prepare an annual report summarising all notifications received by them under this section, and any action taken in response to a notification.

(6) A copy of the annual report must be sent to the European Commission and to ENISA.

Requirement to submit to audit

105C.—(1) OFCOM may carry out, or arrange for another person to carry out, an audit of the measures taken by a network provider or a service provider under section 105A.

(2) A network provider or a service provider must –

(a) co-operate with an audit under subsection (1), and

(b) pay the costs of the audit.

Enforcement of obligations under sections 105A to 105C

105D.—(1) Sections 96A to 96C, 98 to 100, 102 and 103 apply in relation to a contravention of a requirement under sections 105A to 105C as they apply in relation to a contravention of a condition set under section 45, other than an SMP apparatus condition.

(2) The obligation of a person to comply with the requirements of section 105A to 105C is a duty owed to every person who may be affected by a contravention of a requirement, and -

(a) section 104 applies in relation to that duty as it applies in relation to the duty set out in subsection (1) of that section, and

(b) section 104(4) applies in relation to proceedings brought by virtue of this section as it applies in relation to proceedings by virtue of section 104(1)(a).

(3) The amount of a penalty imposed under sections 96A to 96C, as applied by this section, is to be such amount not exceeding £2 million as OFCOM determine to be—

(a) appropriate; and

(b) proportionate to the contravention in respect of which it is imposed.

135 Information required for purposes of Chapter 1 functions

(3) The information that may be required by OFCOM under subsection (1) includes, in particular, information that they require for any one or more of the following purposes--

(ie) assessing the security of a public electronic communications network or a public electronic communications service;

(if) assessing the availability of a public electronic communications network

137 Restrictions on imposing information requirements

(2A) OFCOM are not to require the provision of information for a purpose specified in section 135(3)(ie) or (if) unless—

(a) the requirement is imposed for the purpose of investigating a matter about which OFCOM have received a complaint;

(b) the requirement is imposed for the purposes of an investigation that OFCOM have decided to carry out into whether or not an obligation under section 105A has been complied with; or

(c) OFCOM have reason to suspect that an obligation under section 105A has been or is being contravened