Ofcom
making communications work
for everyone

# Updating Ofcom's guidance on network and service security

## 2017 Summary of consultation responses

**STATEMENT**

Publication Date: 18 December 2017

# About this document

The legislation that applies to telecoms providers requires them to take measures to protect the security and resilience of their networks and services. Ofcom has the power to intervene if we believe a provider is not taking the appropriate measures. In May 2011, we published guidance telling the relevant providers what we expect them to do in order to meet their obligations. We updated this guidance in 2014.

In June 2017 we decided that it was appropriate to make some further updates, and published a consultation setting out the changes we were proposing. This document summarises the consultation responses we received, gives our response to them, and explains the changes we have decided to make as a result. We are also publishing the resulting revised guidance, called 'Ofcom guidance on security requirements in section 105A to D of the Communications Act 2003, 2017 Version', alongside this document.

Telecoms providers sent most of the responses we received, but we also heard from the Information Commissioner's Office. In summary, the providers were primarily concerned that some aspects of the revised guidance would increase the compliance burden on them. Most agreed that some updates would be beneficial, but there wasn't universal agreement that any of the suggestions in our consultation were correct, or indeed incorrect. For the most part, we have decided to proceed with the changes we proposed, in some cases with additional clarification or slight alterations.

# Contents

## Section

# 1. Introduction

1.1 We published guidance on the security obligations in section 105A to D of the Communications Act 2003 in May 2011. The objective of that document was to give providers of public electronic communications networks and services (CPs) high level information we would expect them to take account of in complying with their statutory obligations. In summary, it covered the following areas:

- risk management procedures and basic security measures;
- transparent information for consumers;
- measures to maintain the availability of services;
- measures to protect interconnecting networks; and
- reporting incidents which exceed the thresholds outlined in the guidance.

1.2 In that document, we explained that we expected to revise our guidance from time to time. Following consultation, we updated the guidance in 2014. In June 2017, Ofcom published a consultation regarding further changes to the guidance and asked for comments on our proposed revisions.

1.3 This document summarises the main points made in response to our consultation. It also gives our views on these responses and our conclusions on the changes we have decided to make to the guidance. We are publishing the revised version of the guidance alongside this document.

## Responses

1.4 Ofcom received responses to the consultation from:

- BT
- Colt
- Telefonica UK (O2)
- ICO
- KCOM
- Sky
- Three
- Verizon
- 3 confidential responses

1.5 Copies of the non-confidential responses can be found on our website here: https://www.ofcom.org.uk/consultations-and-statements/category-1/review-security-guidance

# 2. Security & Availability (s105A)

## Cyber security

2.1 In this section of the consultation we proposed the following changes to the guidance, intended to better reflect the importance we attach to CPs' management of cyber threats as part of their section 105A-D obligations:

- explain that managing cyber security risks is an essential part of compliance with section 105A;
- reflect the creation of the National Cyber Security Centre, NCSC, and set the expectation that CPs should be aware of, and where appropriate be following, NCSC's guidance on relevant issues; and
- explain that when investigating and considering enforcement action we will look to NCSC for guidance on any cyber-specific measures CPs should be taking.

2.2 BT set out its view that section 105A(1) is "clearly intended to refer to incidents that affect the network or service availability". It therefore considers our proposal as an extension to the scope of section 105A.

2.3 We disagree with this interpretation and consider, as we have discussed previously[1], that "security" in the context of section 105A(1) includes all three aspects commonly associated with security, namely confidentiality, integrity and availability. This is in line with the interpretation in Government's consultation on transposing the underlying Directive into UK law[2]. We also note that section 105A(4) goes on to state:

*2.4 "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".*

2.5 We therefore do not consider that we are changing or extending the scope of section 105A. We address cyber incident reporting (section 105B) further in a later section of this document.

2.6 One CP stated that following some NCSC guidance is not feasible due to a lack of support from the manufacturers of the equipment it uses. As with the previous versions of our guidance, the publications we reference, such as those by NCSC, are intended to illustrate some of the sources we will use when considering whether a CP has fulfilled its obligations to take measures to appropriately manage security risks. It is for each CP to consider which measures are appropriate in its particular context, taking into account any constraints that may make them impractical or disproportionate. However, just because a particular measure is "not supported" by its current equipment, this doesn't necessarily mean it is not appropriate.

[1] For example, paragraph 3.2 of our current guidance - https://www.ofcom.org.uk/__data/assets/pdf_file/0021/51474/ofcom-guidance.pdf

[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/72835/10-1132-implementing-revised-electronic-communications-framework-consultation.pdf

2.7 Another respondent made the general point that there are lots of bodies with an interest in cyber security compliance matters and therefore potentially conflicting obligations when considering what actions are needed in relation to security. The respondent wanted Ofcom to work to encourage a consistent approach. We acknowledge the complexity in this area and do work closely with other bodies such as NCSC, DCMS, ICO and other EU regulators to ensure as much consistency as possible. Ultimately however, we are not responsible for other potentially conflicting requirements, and can only seek to clarify what we consider is needed for compliance with section 105A and 105B.

2.8 In conclusion, we have decided to go ahead with the proposed changes to the guidance in relation to cyber security, and reiterate that our understanding of "security" in the context of section 105A includes confidentiality, integrity and availability.

## Risk management & governance

2.9 We proposed to make the following changes to better reflect the importance of appropriate governance, and to update our guidance on certification against security standards and the role this plays in risk management:

- explain that when investigating potential breaches, 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;
- emphasise the need for CPs to have a sufficient level of internal security capability to ensure those considering such risks are appropriately informed; and
- explain that although potentially useful evidence in any investigation, certification against any particular security standard is not a requirement for compliance.

2.10 Sky said that they favour a risk management approach based on identifying specific threats faced, designing and implementing appropriate tests that establish whether attacks can be detected, and assessing the efficacy of the steps taken to mitigate those threats. It suggested that such an approach involves continuous learning and improvement. We generally agree that this is a sensible approach. It is essentially the philosophy of the risk-based approach set out in the guidance, and is further supported by the cyber vulnerability testing scheme we discuss below.

2.11 There was general concern relating to the number of security standards that CPs are expected to comply with. One CP expressed concern on the perceived burden, stating that it chose to rely on internal bespoke controls rather than seek external certification. Another made the broader point that guidance is not as effective as regulation and also suggested that Ofcom should put more weight on ISO 27001 compliance.

2.12 Ofcom acknowledges the complex and changing range of activities that a CP needs to undertake in order to maintain appropriate security measures. We already address the value of ISO 27001 in the existing guidance and continue to consider that it is important; we do not intend to change this aspect. However, there is no one standard which covers all aspects that we consider are relevant when assessing whether a CP has met its obligations to take appropriate security measures. The changes proposed in the consultation are intended to keep the compliance requirements proportionate by clarifying that formal certification against an ever-growing range of standards is not required in order to be compliant. However, CPs nonetheless need to determine and maintain the relevant controls and procedures to appropriately address the security threats they face.

2.13 In conclusion, we will make the proposed changes to the guidance in relation to appropriate governance, and to clarify the role of standards certification in our assessment of compliance.

## Cyber Essential Plus

2.14 We proposed updating the guidance in relation to the Government's Cyber Essentials Plus scheme:

- while we will continue to consider that the controls in the scheme are important for CPs to consider, it may be disproportionate for some CPs to seek certification.

2.15 More than one CP queried the suitability of applying Cyber Essentials or Cyber Essentials Plus to them. Some stated that the scheme was designed for Small to Medium Enterprises rather than large telecoms operators, and therefore achieving certification can be difficult.

2.16 These points are supportive of our proposed changes to the guidance to note that certification may not proportionate for all CPs. We will therefore go ahead with the proposed changes.

## Minimum Security Standard for Interconnection – NICC ND1643

2.17 In this section, we proposed updating our guidance to reflect our expectation that NICC would shortly be revising ND1643, and changing its status from a certification standard to best practice guidance.

2.18 Several CPs requested confirmation that ND1643 was still required as a standard by Ofcom and some questioned whether it was still relevant.

2.19 We believe that the work undertaken by NICC to update the document should address any concerns about its continued relevance. The change in status from a certification standard to guidance will automatically mean that it will longer be meaningful for Ofcom to encourage certification.

2.20 Since we published the consultation, NICC has continued its work to revise ND1643. We understand it will, as anticipated, shortly publish the revised document as "guidance", and therefore we have updated our own guidance accordingly.

## Cyber vulnerability testing

2.21 We explained the cyber vulnerability testing framework used by the Bank of England, and expressed our support for a DCMS-led project to develop a similar scheme for use by CPs, which is currently being piloted.

2.22 Both Colt and Sky recognised the value of such a scheme and expressed a desire to participate as and when it is formally introduced. The ICO were also supportive of this approach.

2.23 There were concerns raised about the use and integrity of sensitive information associated with such a scheme, and it was suggested that it would duplicate other standards and testing. There were calls for greater clarity on how the scheme would operate in practice, whether it will be mandatory or voluntary, and how testing would be carried out in a live operational environment.

2.24 KCOM said that we should make it clear that information gathered through penetration testing would be used in any enforcement actions. It also stated that wherever possible, any testing should not duplicate measures that form part of other standards.

2.25 During the development of the pilot scheme, DCMS held a number of workshops involving most of the larger CPs, at whom the scheme is expected to initially be targeted. The majority of the issues raised by consultation respondents were discussed during these workshops, and steps were taken in the design of the pilot scheme to address them.

2.26 We appreciate however that not all respondents were involved in these workshops, and even for those that were, some concerns remain. Testing the approaches to address these and other issues is to a large degree the purpose of the pilots which are currently underway.

2.27 We expect that following the pilot there will be a need for further engagement with industry in order address any outstanding issues and finalise the scheme.

2.28 On the specific issue of overlap with other standards, this is an area which has been considered in detail in the industry workshops and subsequently. In most cases, the objectives of the scheme have been found to be distinct from those of existing standards. Where overlap has been identified, work is underway to minimise this.

2.29 Similarly, the potential overlap with CPs' existing penetration and "red team" testing has also been considered in detail. These terms are used to describe a whole spectrum of testing activity employed by CPs to assess the vulnerability of their networks to hostile attack. While there may be some overlap, there are a number of features of the pilot testing scheme that tend to make it distinct from the types of testing that a CP may already be carrying out either to comply with other standards, or for internal assurance purposes. In particular, some relevant features of the cyber vulnerability testing scheme are:

- both the threat intelligence which is used to develop the testing scenarios, and the testing itself, are undertaken by 3rd parties rather than the CP's own staff;

- the ultimate objective of the testing is address potential causes of major disruption to the key services offered by the CP, such as voice or broadband, rather than the more typical system-specific penetration testing approach;
- much of the focus of the scheme is to assess the ability of the CP to successfully detect and response to attacks, rather than just to eliminate common vulnerabilities;
- the testing is conducted on live systems, and is not announced to those operating those systems or monitoring security; and
- the scoping, threat intelligence gathering, testing and remediation phases are all open and transparent between the parties involved, with relevant documents being shared between the CP, Ofcom and Government[3].

2.30 We believe that the type of intelligence-led vulnerability testing used by the scheme should be an integral part of an appropriate approach to managing cyber security risks, as required by section 105A. With such a fast-changing and complex threat, such testing is an important part of a CP's approach to developing and maintaining effective security measures. We are aware that many CPs already undertake various forms of vulnerability testing, but as discussed above, we feel this scheme offer some unique features. As such, we think it has the potential to provide powerful evidence that a CP is taking appropriate security measures in relation to cyber security in the event that we undertake an investigation.

2.31 In conclusion, it remains our view that the scheme has the potential to be a very valuable tool for assessing the levels of cyber security achieved by a CP, and for effectively directing future improvements. We have amended our guidance to reflect this matter.

## Maintaining network availability

### Single Points of Failure

2.32 We proposed to make the following changes to the guidance in relation to single points of failure:

- explain that we consider avoiding single points of failure, where it is reasonably possible to do so, is likely to be an "appropriate step" within the meaning of section 105A(4); and
- note that the extent to which avoiding single points of failure is reasonably possible will vary at different points in the network, and give some examples of relevant considerations.

*2.33* O2 disagreed with the definition we gave of single points of failure and supplied its own. We disagree with its view that a single point of failure can only be such if all of a CP's traffic passes through it. We have however, altered the definition used in the guidance from that in the consultation to provide additional clarity on the meaning of this term.

[3] Although it should be noted that due to the potential security implications of disclosure, much of the documentation will need to be held securely and within a restricted group in these organisations.

2.34 BT agreed with the point raised, stating that "the precautions CPs take must be balanced against the economic cost of doing so". KCOM said that it was right that Ofcom should recognise that the reasonableness of the 'appropriate steps' that a CP is expected to take is a function of the points in a network under consideration.

2.35 Sky raised a question regarding the distinction between protection paths in a CP's backhaul and core networks. Another respondent wanted more clarity and examples, stating that networks were complex.

2.36 We do not consider that we can give any more specific guidance on these matters as each case will need to be judged on the facts. However, an expanded list of factors likely to be relevant in determining whether appropriate steps have been taken has been included in the guidance.

## Flood & Power Resilience

2.37 We proposed updating the guidance with the following changes to better reflect the importance we attach to the appropriate management of the risks to availability posed by flooding and power loss:

- reflect the growing risk to availability posed by flooding;
- explain that we expect CPs to manage the risks of flooding and power loss appropriately;
- explain that flood protection for critical sites, such as single points of failure, should be considered even if the risk of flooding is relatively low; and
- we will be more closely examining the mitigation steps taken by CPs following significant flood and/or power outage incidents, and will launch formal investigations if appropriate.

2.38 O2 took the view that there is no case for regulatory intervention to attempt to force operators to provide greater resilience. KCOM considered that Ofcom should recognise the cost to CPs of mitigations to improve resilience. Another respondent wanted Ofcom to take a proportionate approach to flood and power resilience, with BT stating that the precautions taken by CPs must be balanced against the economic cost of doing so.

2.39 ICO were supportive of our proposed focus and explained that its audits already consider BCP/DR[4] arrangements due to the potential to cause data breaches.

2.40 Colt stated that these risks were understood and mitigated against, and that it works actively within EC-RRG[5] and takes part in exercises.

2.41 We note that changes in our guidance do not change the regulatory obligations for CPs, which statutory obligations are imposed on CPs by sections 105A to 105C. As regards to the response about Ofcom taking a proportionate approach, we note that Ofcom always has regard to (as required by section 3(3)(a) of the Communications Act 2003) the

[4] Business Continuity Plans / Disaster Recovery

[5] Electronic Communications Resilience and Response Group

principles under which our regulatory activities (including our enforcement of sections 105A to 105C) should be transparent, accountable, proportionate, consistent and targeted only at cases in which action is needed.

2.42 With regard to the legislation, section 105A(4) requires that:

*2.43 "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".*

2.44 We consider that this sets a high bar for compliance, and resilience to power and flood risks are two areas of particular concern. We will update the guidance in this area as proposed in order to emphasise this point and explain what evidence we will be seeking during any relevant investigation.

## Outsourcing

2.45 We proposed updating the guidance to explain that:

- outsourcing to third parties does not excuses CPs from their obligations under 105A(4); and
- we expect CPs to check, on an ongoing basis, that actions undertaken on their behalf do not put them in breach of their obligations.

2.46 ICO supported our proposals on this issue and noted the potential issues raised by the trend of reliance on 3rd parties.

2.47 KCOM stated that Ofcom should confirm that the obligations under section 105A(4) cannot be outsourced, but that appropriate outsource arrangements can be used by CPs in providing their networks.

2.48 Citing the example of joint liability in the GDPR[6], Three suggested that Ofcom should clarify when we will use our enforcement powers in relation to 3rd parties. However, as we stated in our consultation, a CP cannot contract out of its statutory obligations under section 105A.

2.49 We will make the proposed changes to the guidance in order to provide clarity on this issue.

[6] General Data Protection Regulation which will come into force in the UK from 25 May 2018

# 3. Incident Reporting (s105B)

## Mobile reporting

3.1 We set out our concerns about the level of incident reporting we have been receiving in relation to mobile services and networks. We proposed a new set of reporting thresholds for mobile, which were intended to meet the objective of significantly increasing the number of mobile of incidents that are reported and achieving more consistent reporting between the operators. We then went on to discuss a proposed approach for calculating customer impact, again with the aim of improving consistency between operators.

3.2 Several respondents commented that the proposed changes, or indeed any changes, to mobile reporting would result in significant costs for mobile operators in establishing and operating the systems and processes required. Concerns were raised that the burden could become disproportionate to any benefit of the increased reporting we are seeking.

3.3 In relation to our proposed thresholds for incidents which should be reported, BT, O2 and one confidential respondent made specific alternative proposals in relation to certain aspects. Typically, these were suggested as they would better fit with the existing systems and processes used by the respondents, hence reducing the cost burden of changing the thresholds. Another confidential respondent expressed the desire to work with Ofcom and other operators to develop "effective and proportionate reporting criteria".

3.4 Several respondents questioned whether the loss of a single technology (e.g. 2G, 3G or 4G) should be reportable, as overlapping capabilities may often mean that customers do not lose service as a result. O2 suggested that instead the focus should be on a loss of a service, such as voice or data.

3.5 O2 disagreed with the proposal to provide a full list of affected sites in relation to reported mobile incidents, arguing this would create an unnecessary burden. It proposed instead that a "simple narrative statement, or basic map snapshot" would suffice. It suggested that a 4 hour disruption was a more appropriate threshold than the proposed 2 hours.

3.6 As has been our approach when establishing mobile reporting thresholds previously, we are again keen to align as closely as possible with existing systems and processes in use by the operators who are likely to need to report in order to minimise unnecessary reporting burdens. However, as we explained in our consultation, the previously agreed thresholds have, in most cases, resulted in a very low level of reported incidents which is in our view, neither sufficiently consistent between operators, nor representative of the volume of significant incidents experienced. We therefore continue to consider that we need to establish new, significantly lower, thresholds for reporting, but do so in a way which does not have a disproportionate impact on the affected operators.

3.7 In relation to the issue of whether the loss of a single technology should be reportable, we agree that incidents of this nature will not necessarily lead to a loss of service for customers. However, we disagree with the implied views of some respondents that this would remove such incidents from being reportable.

3.8 Section 105B sets out several situations which are reportable. One of these is "a reduction in the availability of a public electronic communications network which has a significant impact on the network". In our view, a complete loss of a network technology, such as 2G, 3G or 4G, across a significant number of sites, has clearly had a significant impact on that network.

3.9 In relation to the proposal that mobile incident reports should contain a list of all sites affected, we continue to consider this is a necessary addition. Operators currently provide a range of different information, making it impossible to develop a robust and comparable understanding of the geographic impact of an incident. We consider that operators should already have a list of sites affected by significant incidents, and so the burden of including this information in the incident report should be limited.

3.10 However, as we discuss above, we wish to establish thresholds which result in a reasonable and proportionate level of reporting and some respondents have told us that the particular thresholds we proposed will result in far more reports than we anticipated.

3.11 We welcome the specific proposals on reporting thresholds put forward by some operators, where these are intended to meet the objectives we set out in the consultation while better aligning with the operators' existing systems and processes. We are happy to work with operators to agree reporting thresholds on this basis, and have started a round of meetings to achieve this. We may also hold a workshop for all mobile network operators (MNO) in the New Year, with the intention of comparing agreed thresholds and methods of calculating customer impact to ensure as much consistency as possible.

3.12 In conclusion, we consider that more work with MNOs is required in order to finalise revised reporting thresholds and impact calculation methods. In the revised guidance, we will retain the current approach of explaining that we have individual thresholds agreed with each MNO. However, we have updated in the guidance the description of those thresholds[7] to reflect the mobile reporting objectives we set out in the consultation and the process we are undertaking to revise the agree thresholds in line with these objectives.

3.13 We have also reflected that a full list of affected cell sites is required for relevant incidents, as part of the location information provided in an incident report.

3.14 We intend to closely monitor reporting levels across the mobile sector following establishment of the new arrangements. We will revisit the agreed thresholds and customer impact calculation approach with an operator if we feel its reporting is not as expected.

## Cyber incident reporting

3.15 Several respondents questioned the need to report to Ofcom cyber incidents that related to personal data breaches, as these have to be separately reported to ICO. BT addressed this issue in detail, pointing out that cyber incidents should only "be reported to Ofcom

[7] i.e. the text in Note 5 to Table 2.

under Section 105B when they have *a significant impact on the operation of a public electronic communications network or service*". A similar point was made by Verizon. We agree with this, and indeed made this same point in paragraph 3.29 of our consultation. BT goes on point out that we cannot expand the remit of reporting obligations beyond this. This is clearly right, and it is not the intention of our proposals to do so. The intention of the proposals is to set out the types of incident which we consider are likely to have a "*significant impact on the operation of a… network or service*", and are therefore reportable.

3.16 Verizon suggested that only cyber incidents which result in "network operations outages", and meeting the criteria, would be reportable. We do not agree with the implication that "*a significant impact on the operation of…*" has the same meaning as "an outage of…". From the previous discussion about the definition of "security", a security breach can have a range of consequences. These include a loss of personal data, a loss of other types of data, loss of integrity, and loss of availability. We consider that a major cyber breach resulting in any of these consequences is likely to have "*a significant impact on the operation of a… network or service"* and is therefore reportable.

3.17 In the example of a security breach of a service which leads only to major loss of personal data, this is likely to have profound implications for how the affected CP is operating that service. The steps needed to understand, stop, and prevent reoccurrence of the breach are likely to all be major operational issues, even if the CP manages to maintain service availability for end customers during this process. For example, affected systems such as customer portals, billing platforms or customer devices, may have to be temporarily shut down or have normal operations restricted while investigation and remediation takes place. Software and/or hardware may need to be urgently upgraded or replaced. Similar actions may need to be taken for systems beyond those known to be directly affected. We consider that in such situations, the operation of the service has clearly experienced a "significant impact", even if availability for customers is maintained.

3.18 We highlight here the distinction between a reportable incident under section 105B and a potential breach of the obligations under section 105A. In relation to the latter, each case will need to be considered on its facts to determine whether section 105A applies, or whether, for example it falls under regulations enforced by ICO. This does not, however, alter the fact that, if the impact of the breach on the operation of the network or service is "*significant*", it is reportable under section 105B.

3.19 Situations in which more than one regulation may apply are not unusual. In this document we are considering the guidance we give in relation section 105A-D, however it may be the case that, depending on its specific circumstances, an incident involving a personal data breach engages other regulatory obligations relevant to the telecoms sector.

3.20 In conclusion, we continue to consider that major cyber security incidents should be reported, and we will explain this in the revised guidance as proposed. We will amend the text proposed in paragraph 3.32 of the consultation by adding the word "major", in order to better reflect that only major cyber breaches are likely to have a significant impact on operations and hence be reportable. We will also amend the wording proposed in paragraph 3.45, which says that all cyber incidents should be treated as "urgent incidents", accordingly.

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

3.21 We proposed updating the guidance to reflect a modified version of a reporting process for the most urgent incidents, about which we wrote to the major CPs in December 2015. Alongside this we proposed adopting a new, more specific, 72 hour target reporting period for other incidents, and continuing to accept batch reporting on a monthly basis for "non major" incidents.

3.22 O2 commented on the proposed 3-hour deadline for urgent incidents, and queried our intentions in relation to 24/7 reporting.

3.23 Others expressed concern over the resources required to accommodate the urgent incident reporting proposal and the feasibility of changing existing procedures to accommodate the three-hour timescale. For instance, Sky said that it would require absolute clarity on the definition of an urgent incident, and "accordingly, only clear, quantitative thresholds would be appropriate".

3.24 One respondent strongly opposed 24/7 reporting, stating that this would be disproportionate and would impose a significant burden on its incident management processes. It stated that the time scale is too short and the proposal is more onerous than the requirements in the NIS Directive[8].

3.25 We accept that urgent incident reporting, particularly out of hours, will be a best efforts activity and not always be possible given timing and resource constraints. We would also stress the point in paragraph 3.42 of the consultation that "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". Most large CPs already attempt to quickly notify us in the rare event that they are dealing with a highest priority incident. The proposed change to the guidance is not intended to impose any alteration to such arrangements, but simply to reflect it more formally and ensure all relevant CPs adopt a similar approach.

3.26 We disagree with the suggestion that only quantitative thresholds are appropriate to determine an urgent incident. The qualitative thresholds are all to be applied reasonably however. For example, we are only asking CPs to inform us when they have already become aware of national media coverage - we don't expect CPs to undertake any specific monitoring for the purpose of reporting.

3.27 In conclusion, we will adopt the proposed three incident types. We will modify our description of the "urgent incident" process, to make it clear that what we require initially

[8] Network and Information Systems Directive - https://www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive

is a simple notification of the fact of the incident, with a report to follow according to the normal 72 hour timescale. We will also make it clear that this will be on a best efforts basis.

# 4. Audit & Enforcement (s105C & D)

4.1 We proposed changing the guidance as follows:

- reflect that we may consider exercising the power to conduct audits more often than previously; and
- note that we would still consider the appropriateness of an audit carefully as we are aware they can be a significant burden.
- Reflect that enforcement would follow our separate, published, guidelines.

4.2 Several respondents were concerned about our proposals in relation to audits. One questioned why we would change our current approach, and suggested audits should remain a backstop measure. Several were concerned about the potential burden of auditing. ICO noted the potential for overlap between our audits and its own, and note the need to ensure audits are targeted to risk areas.

4.3 As we explained in the consultation, we are aware of the potential burden of an increased usage of auditing powers. We will continue with the changes proposed in the consultation in relation to audits, and again note that any decision to undertake an audit will be considered carefully on its merits. We have also made specific reference in the guidance to Ofcom's Enforcement Guidelines to remind CPs about our relevant processes, should we decide to take enforcement action.