Updating Ofcom’s guidance on network security

Call for Inputs

Publication date:	13 December 2013
Closing Date for Responses:	21 February 2014

Contents

Section

Section 1

Introduction

1.1 Communications services and the networks that support them must remain secure and operate reliably if they are to satisfy the needs of consumers. These features of a service are often taken for granted and only receive widespread attention when they fail. Consumers may not realise how dependant they and modern life more generally are on these services until they are unable to make a mobile phone call, access the internet, or pay for goods using their credit card.

1.2 The importance of communications services and their continued security and reliability was recognised by legislators when they updated the European framework for the regulation of the sector in 2009. The changes they made were reflected in UK law and came into force in 2011, introducing new obligations on the providers of public services and networks to ensure appropriate security and availability, and to report any significant problems to Ofcom. We in turn received new duties and powers to enforce these obligations. Before these changes, there were few mentions of security or reliability in the legislation, so this represented a new area for both CPs and Ofcom.

1.3 We published guidance on the new security requirements in May 2011, with a minor revision following in February 2012[1]. The objective of that document was to give CPs high level information on how we would apply the new requirements. 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.

1.4 In that document, we explained that we expected to revise it from time to time, and we feel now is the right time to start the process of our first major update. One reason for this is that the broader security environment has changed considerably over the two years since the guidance was published, with concerns about cyber security having come to the fore. Also, the technology and operational practices used in the communications industry have evolved over this time, as has the relative importance of different services. Finally, we now have experience of operating aspects of the existing guidance, such as incident reporting, which suggests some changes would be beneficial.

1.5 This Call for Inputs sets out the areas of the current guidance which we think would benefit from revision, and gives an indication of any particular changes we are considering. We would welcome the views of stakeholders on the value and form of these, or indeed any other, changes to the guidance. We are aware that such changes have potential to add to the regulatory burden on industry, so want to hear stakeholder views before we decide how to proceed. Subject to the responses we receive, we plan to publish revised guidance in 2014.

[1] http://stakeholders.ofcom.org.uk/telecoms/policy/security-resilience/implementation-eu-framework/

Section 2

Legislative framework and current guidance

The European & UK Legislative Framework

2.1 The provision of electronic communications networks and services in the UK is governed by the European regulatory framework. This framework is comprised of a number of separate Directives[2]. Requirements as to network and service security and resilience in Member States are governed principally by Article 13a and 13b of the Framework Directive[3].

2.2 Member States were required to implement Article 13a and 13b in national law by 25th May 2011. In the UK, this was done by revising the Communications Act 2003 (CA2003), principally with the addition of Sections 105A-D. The relevant sections of CA2003 are included in Annex 5.

Ofcom's existing guidance

2.3 Ofcom published our guidance on the security requirements in Sections 105A-D on the 10th May 2011, with a minor revision following on the 3rd February 2012.

2.4 The guidance sets out a number of areas which we expect providers will normally need to have considered in order to demonstrate compliance with the obligations in Sections 105A & B. In summary, these areas are:

- 105A(1) – management of general security risks
  - risk management procedures
  - basic security measures
- 105A(2) – protecting end users
  - transparent information for consumers
  - measures to maintain the availability of services
- 105A(3) – protecting network interconnections
  - measures to protect interconnecting networks, either by compliance with established security standards, or equivalent activity
- 105A(4) – maintaining network availability
  - appropriate steps to protect continuity of supply to downstream services
- 105B – notifying Ofcom of incidents

[2] In particular, 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).

[3] 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.

- processes for reporting incidents which exceed the thresholds outlined in the guidance

2.5 The guidance also sets out our expected use of auditing under Section 105C ("Requirement to submit to audit") and our approach to enforcement under Section 105D ("Enforcement of obligations under sections 105A to 105C").

2.6 We explained that we expected to revise the guidance from time to time to reflect feedback and experience from implementing the new requirements.

Regulatory focus to date

2.7 We have undertaken several activities specifically related to these obligations since they came into force:

- **Reporting** – in order to ensure the UK was able to meet the Commission's deadline of April 2012 for submitting our first annual summary of incidents, ensuring appropriate reporting from CPs was an early priority. We have worked with a number of CPs to agree the details of their reporting arrangements.

- **Infrastructure Report** – In 2011 Ofcom received a new duty to report to the Government on the UK's communications infrastructure. In this document[4], and the two subsequent annual update reports[5], we have included a chapter about the resilience of the infrastructure, drawn from information we have received under Sections 105A & B.

- **Annual summary reports** – we have submitted two annual reports to the Commission, based on a process[6] developed by a working group led by ENISA[7] and comprising the majority of European regulatory authorities. ENISA has published their analysis of these reports for 2011/12 and 12/13 on their website[8].

- **Investigation of incidents** – we have an ongoing programme to investigate incidents that are reported under 105B, or that we otherwise become aware of. We prioritise incidents which appear to be particularly unusual or concerning, which may provide information that can be shared with other CPs, or which have caused high levels of public interest.

  Typically we start these investigations by requesting additional information about the incident, and looking for evidence that the CP concerned took appropriate steps to avoid the incident occurring. We then consider the management of the incident and subsequent steps that have been taken to recover and avoid reoccurrence.

- **Interconnection security** – Article 13a, and in turn Section 105A, include network interconnections between CPs as one of the specific areas that must be appropriately protected. In the UK, the potential for interconnections to expose

[4] http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/broadband-speeds/comms-infrastructure-report/

[5] The 2013 update: http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/broadband-speeds/infrastructure-report-2013/

[6] https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-on-incident-reporting-v-2-0

[7] European Union Network and Information Security Agency

[8] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports

CPs to security threats had already been identified as a concern, and work to address it was underway before the new obligations came into force. In particular, the NICC[9] was working on a standard, ND1643, specifying the minimum security measures required to protect interconnects.

Our guidance set out our strong preference for CPs to demonstrate compliance by obtaining independence evidence of compliance with ND1643 and we have continued to focus on this area. The majority of larger CPs now have certification or plans to achieve it within a reasonable time frame.

- **Outsourcing of network management and/or operations** – the trend to outsource greater proportions of a CP's operational functions to third parties raises potential security concerns under 105A. We have therefore been working with a number of CPs to understand their plans and the steps they are taking to ensure appropriate levels of security are maintained.

[9] Network Interoperability Consultative Committee – the independent technical forum for the UK communications sector that develops interoperability standards for public communications networks and services. http://www.niccstandards.org.uk/

Section 3

Updating our guidance

Experience with the existing guidance has suggested areas that may benefit from revision

3.1 Prior to Sections 105A-D in 2011, Ofcom's involvement in security and resilience issues was limited. Formal security obligations were also largely a new area for CPs, although most were already addressing these issues on a commercial basis.

3.2 The lack of previous experience with the obligations was a driver for the publication of Ofcom's existing guidance, as was the need to define thresholds for reporting "significant incidents" and set out how the reporting process would work.

3.3 With the new obligations having now been in place for over 2 years, we have gained considerable experience in enforcing them. This has suggested gaps in the current guidance which could usefully be filled and other areas which may benefit from increased clarity. In relation to reporting, there are a number of refinements to the current process which may be beneficial.

The importance of telecoms and the expectations placed upon it continue to increase

3.4 The increasing reliance of modern society on electronic communications services was part of the rationale for the security and resilience obligations added to the Framework Directive in 2009. There are no signs that this trend will reduce in the near future. One striking example is the rate at which established activities, from shopping and banking, to socialising and entertainment, are moving online.

3.5 The intense debate in the last few years about the geographic coverage of services such as superfast broadband and 3G and 4G mobile demonstrates their importance. It also suggests that people increasingly expect them to be universally available.

3.6 Although coverage is a critically important part of the debate and has captured the headlines, this alone is not sufficient to successfully deliver the services modern consumers demand. The technical performance of the services, which we refer to as 'quality of experience' (QoE), is receiving increasing attention alongside ongoing work to improve coverage. For example, we have been measuring and publishing fixed broadband speeds data for several years, and have consulted on suitable consumer QoE measurements for mobile data and voice services[10]. While it may not always be as apparent to end users, the reliability and security offered by services can be another important influence on the overall consumer QoE.

3.7 The relative importance of different services has also developed rapidly. For example, the reporting thresholds we set in our 2011 guidance contained seven separate triggers for voice service outages and only one for data – this already feels outdated just two years later.

[10] http://stakeholders.ofcom.org.uk/consultations/mobile-voice-data-experience/

The communications industry, and the security and resilience threats it faces, are changing

3.8 Another driver for revisiting the existing guidance is the pace of change within the communications industry. Communications is driven by a high rate of technology change, arguably more so than any other regulated sector. This can lead to services for which we have provided security guidance, or set reporting thresholds, to be become outdated or replaced by newer ones.

3.9 Competition in the sector also leads to new business practices which can change the types of security risks that CPs face. The factors which CPs must consider in order to ensure they are taking suitable protective steps will therefore evolve over time. The guidance will need to be regularly reviewed to reflect this.

3.10 Outside the CPs themselves, the security concerns in the environment in which they operate have changed even in the short time since guidance was published. Perhaps the greatest change of relevance to Sections 105A-D is the increase in concern about cyber security vulnerabilities and threats.

3.11 In November 2011, the Government published the UK cyber security strategy[11], and committed £650m to the National Cyber Security Programme (NCSP) over the following four years. The NCSP is focused on achieving four objectives by 2015:

- the UK tackling cyber crime and being one of the most secure places in the world to do business in cyberspace;
- the UK being more resilient to cyber attacks and better able to protect our interests in cyberspace;
- the UK having helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies; and
- the UK having the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives.

3.12 We need to be mindful of this broader UK and international security context as we consider Sections 105A-D; although the obligations do not mention cyber security directly, there are clear links to some of Government’s objectives and work under the NCSP. We will continue to work with Government to understand their concerns and the work they are undertaking to address them. Although limited in scope, the role of Sections 105A-D in relation to cyber security is material and our approach must take the wider landscape into account.

Security and resilience vulnerabilities in the UK’s telecoms networks – a review by Detica

3.13 During the drafting of the 2011 guidance, we found a relatively large amount of information about what might be considered “traditional” risks posed to communications providers. These include risks such as dependency on a reliable electricity supply, infrastructure vulnerability to damage during severe weather events, and the impact of hardware failures. These are issues which have affected CPs for as long as they have operated networks and services. Some of these risks

[11] https://www.gov.uk/government/publications/cyber-security-strategy

will develop over time, for example it is predicted we will see more frequent and more severe extremes of weather due to climate change. While these types of risk will always continue to cause problems and on occasion overwhelm the protections that CPs have invested in, these protections are generally well understood.

3.14 Significant amounts of attention have also been paid to the risks, both traditional and more contemporary, posed by deliberate threats, such as criminal or state-sponsored actors. Tackling cyber security threats in particular has been the focus of a lot of Government resources over the last few years.

3.15 We have seen less evidence of existing work considering whether the industry is likely to be facing any new risks, either now or in the future. Given the rate of change in both the technology that underpins networks and services, and the business practices used to operate them, we are concerned that traditional topics like power resilience and building access controls may not be sufficient to deal with all the risks CPs may be facing.

3.16 It is particularly difficult to predict new problems which may occur but which have not yet been observed. However, simply focussing on tackling well known problems could leave potential new weaknesses unaddressed until it is too late. We therefore feel that it is important to maintain a forward looking approach.

3.17 To explore this in more detail, we commissioned Detica to conduct a review of the topic. Their work considered vulnerabilities that currently exist and also attempted to anticipate potential future vulnerabilities that may develop based on current industry trends. Three examples from their report:

- increasingly ageing infrastructure used in the network, including components that are no longer supported;

- a lack of complete understanding of internal network interconnections and dependencies, making incidents more likely to occur and to have a larger impact when they do; and

- less resilient equipment as a result of vendors attempting to deliver core requirements at the lowest possible cost as CPs drive down their service provision costs.

3.18 Detica's report is published alongside this Call for Inputs[12]. We would welcome views on the current and potential future vulnerabilities it identifies and whether additional guidance is required on appropriate measures to address the most serious.

Question 1 – What are your views on emerging and potential future security and availability risks and whether they should be addressed in the revised guidance?

Purpose of this Call for Inputs

3.19 In our 2011 guidance, we explained that we expected to make revisions from time to time to reflect feedback and experience from implementing the new requirements, and address any relevant changes in the security environment.

[12] http://stakeholders.ofcom.org.uk/binaries/consultations/cfi-security-resilience/annexes/detica-report.pdf

3.20 We feel that we have gained sufficient experience, and have seen sufficient changes in the environment, to warrant a revision to the guidance in the coming months. Through this Call for Inputs, we are inviting contributions on the specific issues we raise here, and also on any other matters which stakeholders feel may be relevant to the guidance.

Section 4

Security and availability

Introduction

4.1 This section considers Section 105A of CA2003, which covers obligations to protect the security and availability of networks and services.

4.2 Each subsection starts with a brief summary of the main elements of our existing guidance. This is followed by a discussion of areas which we are considering for revision and our current thinking about the changes we may make. For each, we would welcome comments on the issues we have raised and any additional areas which should consider.

Section 105A(1) – Management of general security risks

Summary of current guidance

4.3 **Risk management** – as a minimum, periodic consideration of main security risks to networks and services and implementation of a plan for appropriate mitigation.

4.4 **Basic security practices** – compliance with a general information security standards such as ISO270xx, and/or other evidence that good practice is followed, such as:

- documented security policy;
- security agreements with third parties;
- documented security roles and responsibilities;
- employee screening and contractual obligations;
- management of technical vulnerabilities;
- access controls; and
- reporting and management of security incidents.

Management and technical expertise

4.5 Perhaps the most straightforward approach to demonstrating that security and resilience have been appropriately addressed is audited compliance with the controls set out in a security standard. This topic is discussed in the following section, as we think including such standards-based controls in our guidance can be helpful in setting expectations. However, ultimately we can only judge whether the 'appropriate' security measures have been taken on a case by case basis. This will usually mean we will be looking more broadly than a simple checklist of security controls.

4.6 Auditing against security standards tends to focus on establishing whether a CP has the right processes and documentation in place for each of the controls. Regulatory guidance will typically follow a similar path, as this approach gives measurable objectives against which compliance can be assessed. While this approach can provide a good deal of assurance, the appropriateness of a CP's security is ultimately difficult to judge externally. It is important that the capability to assess and implement security across the organisation is maintained, which requires suitable skills at both management and technical levels. For example, determining exactly which security controls are important, and how they are best addressed, can only be done with consideration of a CP's specific circumstances. This can't be done effectively if the CP doesn't have the capability to do so. Therefore, alongside the standards-based controls discussed below, we strongly encourage CPs to ensure they have appropriate organisational expertise to discharge their security responsibilities.

Security controls

4.7 At the highest level, we expect CPs to adopt established security practices, and some key examples of this are reflected in the existing guidance. If a security standard existed which closely aligned with the requirements of section 105A, this would potentially simplify matters. CPs could satisfy themselves they were compliant by seeking third party audit of their activities against the standard, and Ofcom could use the auditor's report to do likewise. However, work done for the Government when these obligations where added to the Act, and a subsequent review performed by ENISA[13], suggests no such standard exists.

4.8 Even ISO27002 and 27011 which are mentioned in the existing guidance and are perhaps the most established security standards across the telecoms industry, do not map directly to the requirements in section 105A. They cover only the security of information assets, and consider the risks to the organisation itself, rather than its customers. In other areas, the standards cover more areas than 105A and with over 100 controls, gaining certification may be unrealistic for smaller CPs.

4.9 The Department for Business, Innovation and Skills (BIS) has recently announced[14] its intention to work with industry to develop a new implementation profile based on the ISO27000 series standards. This is the outcome of work to look for a cyber security standard that would be accessible for businesses looking to follow best practice in basic cyber hygiene and to mitigate cyber risks at low threat levels. We will monitor the resulting profile as it is developed and consider its suitability for Section 105A(1). Our current understanding is that as it will be designed as a basic level standard for general businesses, its contents are likely to be necessary, but not sufficient, steps to demonstrate Section 105A(1) compliance.

4.10 In another attempt to address the lack of an "off-the-shelf" standard, ENISA, working with most of the European NRAs including Ofcom, produced a "Technical Guideline on Security Measures" which was published in 2011. Since then, the group has been working on a second version with significant changes and improvements over the original. A final "version 2" is expected to be published in the first half of 2014. In the meantime, a mature draft, version 1.98, is available on ENISA's website[15].

4.11 The current draft of the Technical Guideline document sets out 25 security objectives grouped into 7 domains. These domains, along with an example of a security objective from each are:

[13] https://resilience.enisa.europa.eu/article-13/shortlist-of-networks-and-information-security-standards
[14] https://www.gov.uk/government/consultations/cyber-security-organisational-standards-call-for-evidence
[15] https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/technical-guideline-on-security-measures-v1.98/at_download/fullReport

- Governance & risk management – e.g. security roles and responsibilities;

- Human resources security – e.g. security knowledge and training;

- Security of systems and facilities – e.g. control of access to network and information services;

- Operations management – e.g. change management procedures;

- Incident management – e.g. incident detection capability;

- Business continuity management – e.g. disaster recovery capability; and

- Monitoring, auditing and testing – e.g. security scanning and testing.

4.12 Under each of the security objectives, high level security measures are given which could be taken by a CP to reach the objective. Examples of the evidence that could be provided to an auditor are also included for each measure.

4.13 Three "sophistication levels" are used throughout the document, to group the security measures and evidence that could be applicable to CPs seeking to reach different levels of maturity:

- Level 1 – basic measures needed to meet the security objective;

- Level 2 – industry standard measures, reviewed following any changes or incidents; and

- Level 3 – state of the art measures, backed by a structural review process and proactive steps to improve implementation.

4.14 The Technical Guidelines, while not forming a standard in its own right, has the advantage of being targeted specifically at the requirements of Article 13a (and therefore Section 105A). We feel that in its "version 2" form this document is likely to be very helpful to both CPs and Ofcom in setting out in more detail than our 2011 guidance the range of security objectives that need to be considered.

4.15 We also recognised the benefits of a harmonised approach across EU Member States. There are benefits to consumers and to CPs, especially those operating in more than one country, in the adoption of a common approach. However, there are practical difficulties in finding such an approach due to the material differences in the market conditions and the broader security context in each country. We think the ENISA Guidelines strike the right balance in reflecting good security practice generally, and allowing the benefits of a common approach where this makes sense.

4.16 We are therefore considering updating this section of our guidance to reference the ENISA Technical Guidelines document as the starting point for considering compliance with 105A(1).

Supply chain risk

4.17 Alongside managing internal operational risks, a CP must ensure security is maintained across the supply chain if the overall security of its operations is to be assured. Although this has always been true, it has become of increased importance in recent years as these supply chains have become more complex and new players have become involved, potentially introducing new security risks.

4.18 Much of the focus in supply chain security to date has been on equipment supply and the risks this can present. When properly identified and assessed, these risks can usually be satisfactorily mitigated. Huawei's Cyber Security Evaluation Centre is one example of an attempt to address security concerns about a supplier and its equipment, as explained in the Intelligence and Security Committee's recent report[16].

4.19 Third parties have long been used by CPs for many functions beyond simple equipment supply. Even companies whose core business is equipment manufacture routinely undertake additional activity such as network design, build, management and maintenance for their customers, often for networks involving competitors' equipment as well as their own. This trend is increasing, with some CPs now outsourcing much of what would traditionally have been considered core network provider functions. Such arrangements can give third parties very significant control over a CP's network, which can raise new security concerns.

4.20 Given the increased importance of outsourcing, a CP must be able to demonstrate that it is appropriately managing security risks in its equipment and services supply chain.

4.21 We can identify several general principles which are likely to be relevant across all supply chain arrangements:

- **Risk management** – we would except to see evidence of risk assessment, and the design and implementation of appropriate mitigations, before any significant new supply chain arrangements are entered into;

- **Supply chain management processes** – suitable processes should be in place for the ongoing management of supply chain risks; and

- **Sufficient technical and management expertise** – suitably skilled staff within the CP to ensure supply chain management processes are effectively implemented.

4.22 Beyond these general principles, it is difficult to give specific guidance as to what would constitute an appropriate set of mitigations to the risks arising in each case. We therefore strongly encourage CPs to discuss all material changes to their supply chain arrangements with us well in advance of finalising them. In this way, we can jointly consider any potential security implications, and ensure these are adequately addressed. This will minimise the risk of any future compliance concerns, and the associated risk that additional costs will need to be incurred as a result of mitigations having to be put in place after the event.

4.23 Finally, we note that changes to supply chain arrangements might also have implications for other relevant legislation, such as RIPA and the Data Retention Regulations. CPs should also discuss such changes with the relevant agencies, and do so well in advance of finalising them.

[16] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/205680/ISC-Report-Foreign-Investment-in-the-Critical-National-Infrastructure.pdf

Use of 3rd party data centres

4.24 Space in shared data centres is rented by many organisations, including CPs, to house computing equipment. For CPs in particular, this may include equipment which is important to the ongoing operation of their networks or services.

4.25 Concerns have been raised by Government that the level of physical security in some data centres may not be sufficient to appropriately address the risks present in such sites. This may be less of a concern for some data centre users with less critical requirements, but may raise issues of compliance with 105A(1) for those providing communications networks and services.

4.26 The existing guidance points to ND1643 for appropriate minimum security measures for shared sites and this standard includes controls for physical security. However, its scope is unlikely to cover all uses of data centres by CPs, and the controls may not be sufficient to address the specific concerns that have been raised.

4.27 The revised guidance could attempt to address this issue by suggesting specific examples of mitigations that we would expect to be used to ensure appropriate levels of security are maintained. However, if these mitigations include improvements to physical security that can only be undertaken by the landlord of the data centre, it is unclear how much influence a given CP would have. The practical impact of such an approach may be that a CP either can secure improvements under its existing contract, or perhaps can no longer use particular data centres at all.

4.28 An alternative approach might be for Ofcom or Government to engage directly with the owners and operators of these data centres, with the objective of improving physical security. These approaches and their outcomes could have very different cost and proportionality implications for CPs, and we will take this into account in our final guidance.

Smaller CPs

4.29 As discussed in the previous section, most of our regulatory activity around Sections 105A-D has so far focussed on larger CPs. We have prioritised our activity in this way as it allowed us to quickly form a view of security, resilience and reporting matters across a large proportion of the UK's consumers.

4.30 With the Sections 105A-D obligations now more established, we feel it is the right time consider in more detail how they apply to smaller CPs. It is clear that many of the measures by which a major national CP is judged would not be appropriate for a small local CP. However, among its customers, the security and resilience of a small CP are just as important as they would be for a large CP. Also, the inherently interconnected nature of telecoms networks means that failings in any CP, however small, can have an impact across many others.

4.31 The ENISA Technical Guidelines attempts to distinguish between different CPs on the basis of their "sophistication levels" and this may be a useful tool when considering the compliance of a smaller CP.

4.32 As well as determining the security measures that are appropriate for them to take, any guidance we issue aimed at smaller CPs must be proportionate to their activities and the risks they and their customers face. We would therefore encourage CPs with which we have not yet discussed Sections 105A-D, to contribute their views on this document.

4.33 However, there are practical issues in engaging with the hundreds of CPs that are potentially covered by Sections 105A-D. There are resource implications for both Ofcom and particularly the CPs themselves, many of whom may not have dedicated regulatory or security staff. Cooperation with relevant trade bodies is therefore expected to be an important part of our engagement. In addition, we will also test demand for Ofcom hosted workshops to introduce the obligations in Sections 105A-D and discuss the revision of our guidance.

Question 2 – In relation to the obligations to manage general security risks, how should our guidance be revised to reflect issues such as ENISA's Guidelines on security controls, supply chain management, the use of 3rd party data centres and applicability to smaller CPs?

Section 105A(2) – Protecting end users

Summary of current guidance

4.34 **Access to the emergency services** – detailed requirements for services offering such access are contained in GC3 and GC4[17].

4.35 **Transparent information for consumers** – appropriate measures should be taken to ensure the level of security offered by a service is communicated to consumers and is delivered as promised.

4.36 **Maintaining the availability of services** – appropriate measures, to the extent technical and commercially feasible, to protect the security of services, including their availability.

Risk management and transparency

4.37 Adopting good security practices, as discussed in the previous section, will have a significant contribution to ensuring that end users are appropriately protected. In general, measures which protect the security of networks and services will also protect their end users. However, as 105A(2) is an additional specific requirement for end users to be protected, we expect CPs to be able to demonstrate how they have taken this into explicit consideration in their assessment and mitigation of risk.

4.38 A CP may not be able to perform a risk assessment which applies to all end users, because even across a single service their needs and circumstances are likely to vary widely. As set out in our existing guidance, end users should therefore have access to accurate information about the security of services and networks, to allow them to make informed purchasing decisions.

4.39 Relevant information in this context can be divided into two categories: information about a CP's approach to securing a given network or service, and information about how well it has actually performed in practice. In terms of a CP's approach to protecting end user security, it is clear that managing security is a complex topic. Therefore establishing information about the approach that would actually be meaningful to end consumers, beyond just the most security literate large businesses, may be difficult.

4.40 As discussed in the later section about availability, statistics allowing performance comparisons between CPs can be helpful to inform consumers and incentivise

[17] http://stakeholders.ofcom.org.uk/binaries/telecoms/ga/general-conditions22nov12.pdf

improvement. Alternatively, information about individual security incidents could be considered for publication. However, in both these cases it may be difficult to produce information that is accurate and meaningful for the typical consumer. We would welcome any suggestions on the practicality and usefulness of publishing additional data.

Question 3 – How best can risks to end users be considered by CPs and appropriate security information be made available?

Section 105A(3) – Protecting network interconnections

Summary of current guidance

4.41 **Compliance with NICC ND1643 standard** - certification against ND1643, or evidence ideally in the form of 3rd party audit, of alternative activities that achieve the same level of protection.

Maintaining progress

4.42 Our current view is that the approach to this obligation set out in the 2011 guidance remains the right one. We are therefore not considering major changes, but there are a number areas which we would like to progress in the coming months.

4.43 Adoption of ND1643 has increased considerably over the last 12 months, with most of the large CPs with which we have been actively engaged now either certified against the standard, or implementing a firm plan to achieve this objective. This is a welcome development and goes a long way to reducing the security risks associated with network interconnection.

4.44 The standard itself, and in particular the accompanying guidance for auditors, was designed to be flexible enough to be applied across both small and large CPs. Despite this, we are not aware of any smaller CPs who have achieved or are seeking certification. We think this should be addressed as we extend the focus of our enforcement activity beyond the larger CPs.

4.45 One approach would be to support a number of smaller CPs through the process of obtaining certification, to confirm the standard is suited to the needs of such companies. We plan to pursue this approach, but would welcome other thoughts on how we can further increase adoption of the standard.

4.46 An area that is outstanding from 2011 guidance is revising ND1643 to extend its scope from just IP interconnections to other technologies such as PSTN. In practice, some CPs have already asked their auditors to consider other forms of interconnect, but we remain of the view this should be formally reflected in the standard. We have therefore asked NICC to address this and we will be working with industry to progress an updated version.

Section 105A(4) – Protecting network availability

Summary of current guidance

4.47 **Suitable levels of availability** – CPs should have evidence that they have considered the requirements of consumers and provide a suitable level of availability.

4.48 **Compliance with GC3 for emergency services access** – the requirement to protect the availability of networks allowing access to the emergency services is dealt with separately under General Condition 3.

Availability information

4.49 The 2011 guidance set out our view that the range of services and consumers supported by different networks varies so widely it is difficult to provide generalised guidance on the “appropriate steps” that should be undertaken to protect availability. As with 105A(2) and the protection of end users, the provision of accurate information is important in this context.

4.50 Many CPs provide information to consumers on the status of their services, and details of outages and when they are expected to be rectified. The completeness of this information and the amount of detail provided appears to vary quite widely.

4.51 The availability of high quality information of this type from CPs to consumers is certainly important in the context of 105A(4). However, we believe it may be best to refrain from attempting to specify exactly what information is provided and in what form.

4.52 Consumer preferences are changing rapidly as is the enabling technology, which has resulted in rapid innovation in this area. For example, the use of real time platforms such as Twitter, which allow direct interaction with consumers, has grown even since our previous guidance was published. Setting out a preferred approach risks impeding this innovation which may otherwise lead to higher quality information for end users. However, we will continue to monitor the information that is being provided, and if we have concerns that the market overall, or a specific CP, is failing to provide appropriate information we will consider further intervention.

4.53 In addition to information provided to end users directly by their CP, it may be that publishing comparable information on the availability of different CPs’ networks would be useful. This would be a similar approach to the data we published on broadband speeds[18]. Such information may drive greater awareness among consumers of the importance of reliable networks, and in turn could create competitive pressure on CPs to improve performance. However, generating genuinely comparable and fair availability data may be difficult. The data we already receive as a result of Section 105B reporting is not intended to provide statistics on the overall availability performance of a network and it would be difficult to adapt it for this purpose.

4.54 An example of how comparable availability data could be generated is in a proposal currently being considered by the FCC in the US[19]. If implemented, this proposal would see mobile network operators required to submit data on the percentage of their basestations that remain operational during and immediately following an emergency in a particular area. Under its proposals, the FCC would make this information publicly available on the basis that it would provide consumers with useful comparative information when choosing a supplier and may incentivise improvements in network resilience.

[18] http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/broadband-speeds/fixed-line-broadband-perf-updates/

[19] http://transition.fcc.gov/Daily_Releases/Daily_Business/2013/db0927/FCC-13-125A1.pdf

ENISA Technical Guidelines

4.55 The ENISA Technical Guidelines[20] discussed earlier contain two security domains which are relevant to the protection of network availability. In summary, these are:

- Incident management – this covers the detection, response to, and communication about incidents; and

- Business continuity management – protecting services from the effects of major failures of information systems, or disasters, and ensuring their timely resumption.

4.56 These are examples of where the ENISA document helpfully considers areas relevant to Section 105A which are not typically included in more general information security standards.

4.57 It may be useful to reflect the associated security objectives and measure presented in the ENISA Guidelines in our revised guidance. This would provide more information to CPs on the evidence we expect them to have available in the event of investigation about network availability.

Question 4 – Should Ofcom consider additional guidance in relation to network availability and the provision of related consumer information?

[20] https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/technical-guideline-on-security-measures-v1.98/at_download/fullReport

Section 5

Incident reporting

Summary of current guidance

5.1 Our current guidance sets out the process for reporting significant incidents. This includes a reporting template giving the types of information we require for each incident. Both quantitative and qualitative thresholds are given to help CPs determine which incidents should be reported. In terms of quantitative thresholds, the minimum number of customers and the duration of an incident to trigger reporting is considerably lower for services providing 112/999 access than for other services. This reflects the particular importance of these services.

5.2 We have included a high level summary of the reports we receive in our Infrastructure Report publications. During the last reporting period, we received 641 reports for fixed services, and 19 for mobile services.

General Issues

Downstream and "over the top" service outages

5.3 Most incident reporting occurs when the quantitative thresholds in our 2011 guidance are breached. These thresholds are based on the length of service interruption and the number of end customers affected. Establishing these figures can be problematic for a network operator if the end users receive service via a downstream CP to which it provides network access on a wholesale basis. In this common situation, the CP operating the failed network may not have complete visibility of the duration or scale of end customer impact. Where we have discussed this with CPs, we have asked them to report based on their best estimate of the end customer impact. This approach appears to have been reasonably successful, but may have led to some under reporting.

5.4 Another situation which may have led to some under reporting is when the network of the upstream CP is still operating correctly, but they are aware that a downstream CP has experienced a service failure affecting end customers.

5.5 A general principle can be given which would apply across these situations, and related ones which we may encounter in the future:

- A CP should report all incidents it has both visibility of and reason to believe may exceed the reporting thresholds for end users it directly or indirectly supplies, regardless of where in the supply chain the incident has occurred.

5.6 There are three example situations which we think could be usefully included in the revised guidance to illustrate this point further:

- A CP supplying a network or service to one or more downstream CPs (for example through wholesale agreements) experiences an incident. The CP should make its best assessment of the number of end users affected as a result. If this, and the duration of the incident, puts it above the reporting thresholds, the incident should be reported;

- A CP supplies its end user customers with additional services fulfilled by other CPs. If the CP becomes aware that one of these additional services has failed, it should make its best assessment of the number of its end users affected as a result. If this, and the duration of the incident, puts it above the reporting thresholds, the incident should be reported; and

- A CP's end user customers use additional services over the top of the network or service it provides, but without its direct involvement. We would not expect the CP to monitor or report any incidents affecting such additional services.

5.7 This is not intended to be an exhaustive list of possible supply arrangements, but does cover the main ones for which reporting questions have arisen so far.

Network and complaint monitoring

5.8 One class of incident which can cause a high level of complaints is localised, often rural, outages which take a long time to be resolved, or persistently reoccur. Some of these may not be reported to us, despite having exceeded the reporting thresholds. In other cases, we have investigated such outages even where the quantitative thresholds have not been exceeded, because the level of complaints suggests they are nonetheless "significant".

5.9 Among these cases, there have been some where the CP involved has been unaware of the incident, or at least has not fully appreciated its scale or duration. While no system of network and service management is likely to identify all problems, it is of concern if significant incidents go unreported, and more importantly unfixed, because they are not correctly detected or flagged for resolution.

5.10 CPs need to have sufficient management oversight of their networks and services to quickly identify significant security and availability incidents. This oversight may involve monitoring of internal signals, such as from equipment fault alarms, and also external signals, such as customer complaints.

Question 5 – Would it be useful to clarify our expectations around reporting in the case of wholesale and "over the top" arrangements, and the need for CPs to maintain sufficient fault monitoring?

Thresholds

5.11 The 2011 guidance sets some quantitative thresholds for reporting incidents to us, along with some more qualitative triggers. By far the lowest quantitative thresholds are for failures affecting 999/112 access, and for the reasons set out below, this has led to far higher numbers of reports related to fixed services compared to mobile. The existing thresholds also tend to mean we only receive reports from the largest CPs, and also don't hear about outages of new services not explicitly listed in the guidance.

Mobile

5.12 When a customer's fixed telephone service fails, it is usually reasonably clear that their ability to use the service to access the emergency services via 112/999 is also lost. If such an incident affects more than 1,000 customers and lasts for more than hour, it will be reported under the existing thresholds.

5.13 For mobile telephony, the situation is more complex. Due to existence of emergency roaming[21] a fault with the customer's own network may not affect their ability to call the emergency services. Mobile outages are therefore not usually reported until they reach the higher quantitative thresholds, such as 10,000 customers for 24 hours. This results in us receiving far fewer reports of mobile outages than we do for fixed, which is not necessarily representative of the fault rates across the network types.

5.14 It is clear that mobile services are for many consumers at least as important as fixed. The European Framework acknowledges this by imposing the same requirements for emergency services access on mobile and fixed networks. In the UK, there are now considerably more calls made to 999 from mobile phones than from fixed. While this facility may be protected by emergency roaming, this may not always be the case.

5.15 The fault that causes the failure of a consumer's home network may be common to other networks in the area, and if so, emergency roaming will not function. One common example would be a power failure affecting all networks in an area. Additionally, the increased sharing between mobile CPs of network elements, such as backhaul connections, masts and even whole Radio Access Networks, increases the risk of common failures. As these incidents currently go largely unreported, we are unable to judge whether or not emergency roaming actually provided protection for consumers.

5.16 Beyond emergency services access, it is similarly difficult to argue that most consumers are less concerned by significant incidents affecting mobile services. It is therefore important that we have sufficient visibility of such incidents. This could be achieved by asking mobile CPs to ignore the effect of emergency roaming when assessing the scale of an incident, and setting the mobile thresholds to match those of fixed.

5.17 Some CPs have explained that it is more difficult to estimate how many consumers are affected by a mobile outage than a fixed one. On fixed networks the number of customer connections is essentially static and therefore known, but when a mobile network has failed, visibility of how many consumers would otherwise be connected at that point in time is lost. Our advice in such situations has been to make a reasonable estimate based on typical traffic patterns recorded when the network was operating correctly.

5.18 An alternative approach, which some CPs have indicated they would prefer, would be to take a network infrastructure based approach to setting mobile reporting thresholds. We think there may be merit in this approach, particularly for infrastructure in the local access network. Alongside revising the thresholds based on customer numbers, we are also considering introducing a requirement to report mobile outages affecting a local area. For semi-urban and urban areas, this might include outages where three or more sites in the same area have failed, and for rural areas, where failures at one or more sites means the majority of a given town or village has lost service.

5.19 Another question that has been raised for mobile services is whether we expect incidents affecting machine-to-machine (M2M) services to be reported. The current thresholds are based on the number of "retail customers" affected by an incident, implying that M2M services would be excluded. Given the potential importance of these services over the coming years, it may be preferable to include them. Revising

[21] Emergency roaming is the ability for a mobile customer to make emergency calls on other networks when their own is unavailable: http://consumers.ofcom.org.uk/2009/10/connecting-citizens/

the thresholds to consider the number of “end users” or “service end points” affected in place of “retail customers” would be one approach to achieve this.

Internet access and other services

5.20 The majority of the quantitative thresholds given in the 2011 guidance are related to voice services, with just one for “internet access” which is set at the high level of 100,000 customers for 24 hours.

5.21 There are several reasons to consider revising this position. Firstly, the “internet access” description seems too narrow to fully reflect the range of non-voice activities that consumers typically undertake; “data” or “broadband” are more commonly used to describe such services. Secondly, as illustrated by the fact that voice services can be offered over such connections, the distinction between voice and “internet access” services is increasingly blurred.

5.22 We continue to consider that access to emergency services is a special case, and that the existing lower thresholds for reporting these outages should remain. However, for other uses, there may be an argument for removing the current distinction and setting the same thresholds for voice and data services. This would be in line with the guidance from ENISA on European-level annual summary reporting[22], in which the thresholds are the same for all service types.

5.23 At the European level, there has been discussion of reporting for other services such as e-mail, which are not included explicitly in our current thresholds. The opposing view is that it is more future proof to use only generic service definitions.

Reports from smaller CPs

5.24 Reporting thresholds based on absolute numbers of customers affected will always result in more reports from CPs with larger customer bases. For the smallest CPs, even the complete loss of their service may impact too few customers to trigger reporting under the existing thresholds. However, it could be argued that such a major failure is certainly “significant” in the context of that CP and its customers, and should therefore be reported.

5.25 Setting much lower absolute thresholds would result in more reporting from CPs with a small customer base, but may also result in a disproportionately high number of reports from larger CPs. An alternative is to set some relative reporting thresholds. An example might be that any incident resulting in loss of service to more than 50% of a CP’s customer base should be reported.

5.26 Relative thresholds could replace the existing absolute thresholds, or they could be used together. The latter approach may be more desirable as relying on relative thresholds alone could lead to the opposite of today’s problem: major incidents involving many millions of consumers may not be reported if the CP involved has a sufficiently large customer base.

[22] https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-on-incident-reporting-v-2-0

Degradations in service

5.27 Although not explicitly discussed in the 2011 guidance, it has often been assumed when considering reporting that the thresholds refer to the number of consumers who have lost service altogether.

5.28 However, in the Act, reportable incidents are given only as those which have a ‘significant impact’ on the operation of a network or service. It is possible that a service or network fault could have a “significant impact” on its operation, even if no consumers had experienced a complete loss of service. An example might be a major reduction in the bandwidth of an ISP’s internet connectivity - consumers may still be able to connect to their internet access service, but be unable to perform their usual activities.

5.29 The ENISA guidance on reporting[23] sets its thresholds based on the number of customers ‘impacted’ without specifying exactly what this means. It does raise the idea that for incidents affecting availability, an outage can be ‘complete’ (for instance a network completely down) or ‘partial’ (for instance 50% of calls dropped).

5.30 We believe additional guidance should be included to provide clarity on how to assess incidents resulting in degradation, rather than complete failure, of a network or service.

Other reporting triggers

5.31 Alongside the quantitative reporting thresholds, a number of qualitative criteria are given which may make incidents reportable. In practice, it appears that most CPs are reporting solely on the basis of the quantitative thresholds. There have been a number of incidents for which we have had to request a report, which we believe should have been reported under the qualitative criteria. The most common of these criteria is incidents which the CP is aware are being reported in the media.

5.32 Our current view is that we should give additional weight to the qualitative reporting criteria in the revised guidance, and consider whether there are any additional ones which should be included.

Question 6 – What are your views on the appropriate thresholds for reporting incidents affecting customers of smaller CPs, mobile networks, data services and services suffering partial failures?

Reporting process

Nominated contact point

5.33 Under the current reporting arrangements there have been a number of significant incidents about which we have sought additional information, but that have remained under the thresholds, and therefore have not been reported. In other situations, where an incident report has been received, we have sometimes found that the information it contains is insufficient to answer all our questions. This reflects the fact that it is very difficult to quantify or describe all circumstances under which an incident should be reported, and to specify all the information that may be needed.

[23] https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-on-incident-reporting-v-2-0

However carefully we revise the thresholds and reporting templates, it is likely that we will still face some information shortfalls.

5.34 Where this has happened in practice in the past, we have used our contacts within the relevant CP to request a standard report, or any more specific information of interest. This informal arrangement has worked well, with CPs responding quickly to our requests, which are often urgent in nature.

5.35 It is important that we have the correct contact information for such situations and that this is kept up to date. Although requests for information through this route are expected to remain infrequent, it is also important that our contact point within the CP is aware and ready to receive and act on them. It may therefore be helpful to reflect this in the revised guidance, and set the expectation that each CP will nominate a contact point (or points) for reporting queries, and will update us if this changes.

Reporting template

5.36 The 2011 guidance contains a reporting template and sets the expectation that all reports will use it. In practice, while some CPs do use the template for all their reports, some do not. To date we have been flexible on this point, accepting reports in other formats where this is more convenient for the CP. We have several concerns with the current template and its use, which we are considering addressing in the revised guidance.

5.37 The fields in the current template are quite loosely specified, leaving lots of scope to complete it in different ways or leave some sections empty. Therefore, even where the template is used, there is considerable chance of misinterpretation and gaps in the information that we receive. As previously mentioned, in some cases the template is not used at all, further increasing the chance of a problem.

5.38 We process the various types of data we receive into a form which can be used perform our own analysis, report to Governemnt, and to fulfil our annual European reporting obligations. It is important to ensure this processing is as error-free and efficient as possible.

5.39 The guidance could be revised to address these concerns with:

- **A more tightly specified template**. This would include features such as:
  - fields marked as mandatory/if available/optional;
  - information on the format and amount of information expected in each field;
  - lists of allowable options for some fields; and
  - alignment with the ENISA template[24] for annual European reporting, which was not available when the 2011 guidance was written. For example, this includes a limited list of root causes to which each incident should be assigned.
- **Rejection of non-compliant reports**. Where the specified template is not used, or not completed correctly, we would ask for the report to resubmitted. We note

[24] https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-on-incident-reporting-v-2-0

the exception that some information may be unavailable or subject to confirmation at the time of reporting, especially where a CP is striving to report a major incident quickly.

5.40 We would also be interested in views from CPs on whether the current use of e-mail is the best way to submit reports. Our current view is that, in light of the relatively low number of reports involved, this remains the most appropriate mechanism. Developing and maintaining a dedicated reporting tool or web interface feels unlikely to proportionate unless report volumes increase significantly.

Timeliness of reporting

5.41 Our existing guidance requires reports to be submitted within a few days of the incident, or 24 hours for those with safety of life implications. For the major incidents, we suggest that real time reporting may be considered if the more normal route of invoking the NEAT process[25] is not followed.

5.42 In practice, we have agreed somewhat different arrangements with some CPs, and we plan to revise the guidance in light of our experience in this area. The main points which we wish to reflect are:

- **Reporting of the smallest incidents can be done in regular batches**. Any outage has the potential to be significant for the consumers concerned, depending on its particular circumstances. We therefore continue to believe that the lower reporting thresholds are useful to allow us to build a complete picture of significant incidents.
  In practice however, we have found we have rarely needed to investigate specific incidents reported under the lowest threshold (1,000 consumers/1 hour). This may be because they typically have well understood causes such as isolated equipment failures, localised power cuts or damage to cables, and are fixed under "business as usual" processes. A longer delay between the occurrence of such incidents and their reports has not proved problematic.
  Some CPs therefore hold back the reports of such incidents and provide them in regular batches, for example every two weeks. This approach is likely to be less resource intensive for both the CP and Ofcom. In the event we do wish to investigate an incident which has not yet been reported, we will request an immediate report from the CP, emphasising the importance for an up to date contact point.

- **Major incidents should be reported as soon as possible, and within hours.** Major incidents which have not triggered a NEAT alert, but which have required urgent investigation have been more common than we anticipated when writing the 2011 guidance. In these situations it is important to receive information about the incident as quickly as reasonably possible, even though this is likely to have significant gaps.
  Major incidents are difficult to define, but in the past have included the loss of a large telephone exchange site or mobile services over a large geographic area or for a significant proportion of a CP's customers. They often result in rapid reporting in the mainstream media.
  Faced with such an incident, a CP's focus should rightly be on management and

[25] National Emergency Alert for Telecommunications (NEAT) is a protocol for sharing information among CPs and other organisations such as Government and Ofcom that are members of the Electronic Communications – Resilience and Response group. More details can be found here: https://www.gov.uk/telecoms-resilience

resolution. As noted in our existing guidance, we wish to keep reporting requirements as light as possible to avoid conflicting with this. However, we have found it is important than we are quickly able to obtain the best available information about the reality of the incident, albeit at a high level.

Confidentiality of reports

5.43 The 2011 guidance acknowledges that some CPs may be concerned about the security of submitting reports, which may contain information with commercial or national security sensitivity, over open e-mail. In practice this has rarely been highlighted as a concern, however we would reiterate that more secure communication can be arranged if required.

Question 7 – What are your views on revising the current process for reporting significant incidents?

Enforcement and auditing

Summary of current guidance

6.1 **Investigation triggers** – we may investigate a CP's compliance with its security and resilience obligations for a number of reasons, including significant incidents (whether or not they have been reported) and at our own initiative.

6.2 **Auditing** – we expect to conduct audits infrequently, in cases where we require additional information about a CP's compliance.

6.3 **Formal enforcement** – if necessary we will use our powers, which include issuing binding instructions and, in the case of serious breaches, fines up to £2 million.

Enforcement

6.4 As indicated in our existing guidance, we will undertake formal enforcement action against a CP using our powers if needed. This could include information gathering under Section 135, issuing notifications which include steps that the CP should take to comply with their obligations under Section 96A, and issuing fines under Sections 96A-C. We continue to believe however, that in most cases informal investigation is likely to achieve the desired outcomes more quickly.

6.5 Our experience to date supports this view. In the limited number of cases which have been judged to require more detailed investigation, CPs have cooperated with our requests. This has included sharing detailed information about an incident and its cause, the processes they had in place to prevent the incident and why they weren't effective. Where appropriate, CPs have also shared their plans for reducing the risk of reoccurrence and their progress in implementing these plans. We will continue to use informal investigation in preference to formal enforcement powers where we believe this is the most effective route to achieving a satisfactory resolution.

Auditing

6.6 ENISA and ISACA[26] held a Cyber Security Workshop in June 2013[27], which focussed on the issue of auditing and Article 13b (which is the basis for our Section 105C auditing powers). The discussion highlighted the importance of assessing and improving security performance, and the role that auditing can play in this. We are aware that many CPs already engage third parties to audit various aspects of the security of their operations, in addition to their own internal assessments.

6.7 From discussions with other national regulatory agencies, we know that the approaches they adopt to using the auditing powers in Article 13b differ. In some cases, auditing is used in a way which ENISA refers to as "preventative" in its

[26] An independent global association engaged in the development, adoption and use of knowledge and practices for information systems. It was previously known as the Information Security Audit and Control Association.

[27] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/schemes-for-auditing-security-measures-1/enisa-isaca-workshop-on-security-auditing-in-the-e-comms-sector/

Technical Guidelines[28]. This involves undertaking audits of particular CPs or groups of CPs on a regular basis, often against the expected security controls for a particular domain, such as business continuity planning.

6.8 We are conscious of the potentially significant burden on CPs that auditing imposed by the regulator can represent. Section 105C requires CPs themselves to pay the costs of such audits, and probably more significantly, the internal cost of preparing for and cooperating with the audit process. Our view remains that audits are best reserved for use in specific investigations where we feel other routes have not yielded the information we require to draw accurate conclusions.

6.9 If the circumstances of a particular investigation do suggest the need for an audit, we will use this power. This may be done entirely with our own resource or more likely we would look to work with one of a number of suitably qualified third parties with which we have contractual framework agreements in place.

[28] https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/technical-guideline-on-security-measures-v1.98/at_download/fullReport - section 5.4.3

Section 7

Next Steps

7.1 For the reasons set out earlier in this document, we believe that it would be beneficial if our existing guidance on Sections 105A-D compliance was revised. The feedback we receive from this Call for Inputs should help us develop our current thinking on the areas of the guidance that would benefit from revision and the form that these revisions should take. If arguments are put forward that suggest we should not revise our existing guidance at this time, we will consider these.

7.2 If we conclude that the guidance should be revised, we do not expect to consult further before publishing a new version, around the middle of 2014.

Annex 1

Responding to this consultation

How to respond

A1.1 Ofcom invites written views and comments on the issues raised in this document, to be made **by 5pm on 21 February 2014**.

A1.2 Ofcom strongly prefers to receive responses using the online web form at http://stakeholders.ofcom.org.uk/consultations/cfi-security-resilience/howtorespond/form, as this helps us to process the responses quickly and efficiently. We would also be grateful if you could assist us by completing a response cover sheet (see Annex 3), to indicate whether or not there are confidentiality issues. This response coversheet is incorporated into the online web form questionnaire.

A1.3 For larger consultation responses - particularly those with supporting charts, tables or other data - please email security_cfi@ofcom.org.uk attaching your response in Microsoft Word format, together with a consultation response coversheet.

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

Ben Willis
Floor 3,
Strategy, International, Technology and Economics Group,
Riverside House
2A Southwark Bridge Road
London SE1 9HA

Fax: 020 7981 3333

A1.5 Note that we do not need a hard copy in addition to an electronic version. Ofcom will acknowledge receipt of responses if they are submitted using the online web form but not otherwise.

A1.6 It would be helpful if your response could include direct answers to the questions asked in this document, which are listed together at Annex 4. It would also help if you can explain why you hold your views and how Ofcom's proposals would impact on you.

Further information

A1.7 If you want to discuss the issues and questions raised in this consultation, or need advice on the appropriate form of response, please contact Ben Willis on 020 7981 3000.

Confidentiality

A1.8 We believe it is important for everyone interested in an issue to see the views expressed by consultation respondents. We will therefore usually publish all responses on our website, www.ofcom.org.uk, ideally on receipt. If you think your response should be kept confidential, can you please specify what part or whether all of your response should be kept confidential, and specify why. Please also place such parts in a separate annex.

A1.9 If someone asks us to keep part or all of a response confidential, we will treat this request seriously and will try to respect this. But sometimes we will need to publish all responses, including those that are marked as confidential, in order to meet legal obligations.

A1.10 Please also note that copyright and all other intellectual property in responses will be assumed to be licensed to Ofcom to use. Ofcom's approach on intellectual property rights is explained further on its website at http://www.ofcom.org.uk/about/accoun/disclaimer/

Next steps

A1.11 Following the end of the consultation period, depending on the responses received, Ofcom intends to publish an updated version of the "Ofcom guidance on security requirements in the revised Communications Act 2003" document during 2014.

A1.12 Please note that you can register to receive free mail Updates alerting you to the publications of relevant Ofcom documents. For more details please see: http://www.ofcom.org.uk/static/subscribe/select_list.htm

Ofcom's consultation processes

A1.13 Ofcom seeks to ensure that responding to a consultation is easy as possible. For more information please see our consultation principles in Annex 2.

A1.14 If you have any comments or suggestions on how Ofcom conducts its consultations, please call our consultation helpdesk on 020 7981 3003 or e-mail us at consult@ofcom.org.uk . We would particularly welcome thoughts on how Ofcom could more effectively seek the views of those groups or individuals, such as small businesses or particular types of residential consumers, who are less likely to give their opinions through a formal consultation.

A1.15 If you would like to discuss these issues or Ofcom's consultation processes more generally you can alternatively contact Graham Howell, Secretary to the Corporation, who is Ofcom's consultation champion:

Graham Howell
Ofcom
Riverside House
2a Southwark Bridge Road
London SE1 9HA

Tel: 020 7981 3601

Email Graham.Howell@ofcom.org.uk

Annex 2

Ofcom’s consultation principles

A2.1 Ofcom has published the following seven principles that it will follow for each public written consultation:

Before the consultation

A2.2 Where possible, we will hold informal talks with people and organisations before announcing a big consultation to find out whether we are thinking in the right direction. 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

A2.3 We will be clear about who we are consulting, why, on what questions and for how long.

A2.4 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 to give us a written response. If the consultation is complicated, we may provide a shortened Plain English Guide for smaller organisations or individuals who would otherwise not be able to spare the time to share their views.

A2.5 We will consult for up to 10 weeks depending on the potential impact of our proposals.

A2.6 A person within Ofcom will be in charge of making sure we follow our own guidelines and reach out to the largest number of people and organisations interested in the outcome of our decisions. Ofcom’s ‘Consultation Champion’ will also be the main person to contact with views on the way we run our consultations.

A2.7 If we are not able to follow one of these principles, we will explain why.

After the consultation

A2.8 We think it is important for everyone interested in an issue to see the views of others during a consultation. We would usually publish all the responses we have received on our website. In our statement, we will give reasons for our decisions and will give an account of how the views of those concerned helped shape those decisions.

Annex 3

Consultation response cover sheet

A3.1 In the interests of transparency and good regulatory practice, we will publish all consultation responses in full on our website, www.ofcom.org.uk.

A3.2 We have produced a coversheet for responses (see below) and would be very grateful if you could send one with your response (this is incorporated into the online web form if you respond in this way). This will speed up our processing of responses, and help to maintain confidentiality where appropriate.

A3.3 The quality of consultation can be enhanced by publishing responses before the consultation period closes. In particular, this can help those individuals and organisations with limited resources or familiarity with the issues to respond in a more informed way. Therefore Ofcom would encourage respondents to complete their coversheet in a way that allows Ofcom to publish their responses upon receipt, rather than waiting until the consultation period has ended.

A3.4 We strongly prefer to receive responses via the online web form which incorporates the coversheet. If you are responding via email, post or fax you can download an electronic copy of this coversheet in Word or RTF format from the ‘Consultations’ section of our website at www.ofcom.org.uk/consult/.

A3.5 Please put any parts of your response you consider should be kept confidential in a separate annex to your response and include your reasons why this part of your response should not be published. This can include information such as your personal background and experience. If you want your name, address, other contact details, or job title to remain confidential, please provide them in your cover sheet only, so that we don’t have to edit your response.

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 4

Calls for Inputs questions

A4.1 This section presents the specific questions that Ofcom seeks responses to in relation to this issue.

Question 1 – What are your views on emerging and potential future security and availability risks and whether they should be addressed in the revised guidance?

Question 2 – In relation to the obligations to manage general security risks, how should our guidance be revised to reflect issues such as ENISA's Guidelines on security controls, supply chain management, the use of 3rd party data centres and applicability to smaller CPs?

Question 3 – How best can risks to end users be considered by CPs and appropriate security information be made available?

Question 4 – Should Ofcom consider additional guidance in relation to network availability and the provision of related consumer information?

Question 5 – Would it be useful to clarify our expectations around reporting in the case of wholesale and "over the top" arrangements, and the need for CPs to maintain sufficient fault monitoring?

Question 6 – What are your views on the appropriate thresholds for reporting incidents affecting consumers of smaller CPs, mobile networks, data services and services suffering partial failures?

Question 7 – What are your views on revising the current process for reporting significant incidents?

Annex 5

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).

(2) 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