Updating Ofcom's guidance on network security

Summary of Call for Input responses

Publication date: 08 August 2014

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 to meet their obligations.

In December 2013, we published a Call for Inputs asking for views on whether, and how, we should update our guidance. This document summarises the responses we received, and how we have taken the points raised into account.

We have decided that it is appropriate to make some updates and are publishing the resulting revised guidance, called '*Ofcom guidance on security requirements in section 105A to D of the Communications Act 2003'* alongside this document.

Telecoms providers sent most of the responses we received, but we also heard from a Government department and the UK's information rights authority. In summary, the providers were primarily concerned that 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.

In the revised guidance, we have made some changes to the incident reporting process to improve the quality of information we receive and to reflect the change in the relative importance of different types of services over the last few years. We have made reference to a new European document which provides additional detail about the range of well-established security measures we expect providers to consider. Finally we have included several topics which may pose particular security risks and which we therefore expect providers to take account of.

Contents

Section		Page
1	Introduction	1
2	Call for Input Responses	2

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 communications providers (CPs) high level information on how we would apply the 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.

1.2 In that document, we explained that we expected to revise our guidance from time to time. In December 2013 we published a Call for Inputs, in which we stated we were reviewing the guidance with a view to completing our first major update. The Call for Inputs set out the areas of the guidance which we thought would benefit from revision, and gave an indication of the changes we were considering.

1.3 This document summarises the main points made in response to our Call for Inputs. It also gives our reaction to these points and their impact on the guidance. We are publishing a revised version of the guidance alongside this document.

Section 2

Call for Input Responses

Responses

2.1 We received responses from:

- BT
- ICO
- Three
- 3 confidential responses
- Dept. of Work & Pensions
- KCOM
- Verizon
- EE
- Sky
- Vodafone

General comments

2.2 KCOM felt that it was timely to review the guidance. Several other respondents expressed a reluctance to see major changes to the existing guidance, generally due to the burden that this would impose.

2.3 We believe it continues to be important to keep the guidance under constant review, and that now is the right time to revise it. This is because we now have three years' experience of using the original guidance, and the industry and security environments have evolved. We accept that major changes risk creating undue burden on industry. We have not changed our overall approach to section 105 compliance. We have not pursued all the suggestions in the Call for Inputs, and where we have made changes, we have attempted to do this in a way which will reduce the potential burdens identified in the responses.

2.4 We have rewritten the guidance from scratch. This is primarily to simplify the document and make it clearer what we expect of CPs. The main change in relation to section 105A is the addition of guidance on a small number of areas we identified in the Call for Inputs. We have also made some limited changes to the reporting template and updated the description of the reporting process to better reflect how it has developed in practice. We have also changed some of the reporting thresholds, which will require some CPs to report more incidents, and bring others into scope for the first time.

2.5 BT suggested there was potential for confusion between the terms "security" and "resilience"/"availability" within the guidance. It suggested the guidance should avoid "security" in preference to the other terms. We note that the relevant legislation places obligations on providers in relation to both security and availability, and so it is appropriate that the guidance continues to address both these areas.

2.6 EE and Three pointed out that security and resilience issues are addressed in existing public-private partnerships such as CPNI[1]'s NSIE[2], EC-RRG[3] and TISAC[4].

[1] Centre for the Protection of National Infrastructure – the government agency tasked with providing protective security advice.
[2] Network Security Information Exchange – facilitated by CPNI to allow industry and government sharing of information about the risks facing networks.

We agree that there is relevant work undertaken in these, and other, fora. However, as the respondents acknowledge, there are statutory security and resilience obligations in place and Ofcom is required to enforce compliance. We do not believe that anything in our guidance goes beyond that required to meet these obligations. We contribute to all the named groups, and several others, and will continue to seek to minimise any overlap.

2.7 Finally, several respondents raised the point that Ofcom should publish more information on reported incidents. There appears to be a link to the suggestion from some respondents that they see limited value in the reporting that they undertake.

2.8 We agree that sharing more information back to CPs would be beneficial. To date, we have included limited information derived from section 105B reports in our annual Infrastructure Report updates. This year, we are planning on expanding this section and providing more detail. We will also start sharing the annual summary reports we send to the European Commission, and ENISA[5]'s subsequent European-level report, with CPs that have submitted reports to us. Finally, we also plan to develop a more detailed annual summary of reported incidents to share with CPs.

Question 1 – Emerging security risks

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?

2.9 Several respondents were of the view that it would be difficult for Ofcom to provide guidance on how to address specific risks, or indeed to even reliably identify them. Respondents also pointed out that there are various other sources of security guidance and that Ofcom should focus the overall approach to risk management, rather than providing guidance on how to manage specific risks.

2.10 We broadly agree with these points. The guidance sets outs the areas which we expect CPs to consider, rather than offering specific advice on how they should address identified security risks. We have maintained a somewhat different approach in relation to the protection of interconnections. Here we strongly encourage CPs to seek certification against a UK industry standard, NICC ND1643[6]. ND1643 does include some specific security controls that must be in place for compliance.

2.11 Respondents including DWP, EE and Three stated that the risks identified in the Detica report[7] were not new and were generally well known and managed. It is welcome that CPs recognise and respond to these risks. However, some of the incidents reported under section 105B, and incidents investigated under our other duties, suggest that some of the trends identified in the report do cause practical problems. We intend to continue to monitor emerging risks in order to inform our enforcement activity and future revisions of the guidance.

---

[3] Electronic Communications Resilience and Response Group – an industry chaired group facilitated by the Department for Business Innovation and Skills (BIS). It develops co-operation between industry and government on telecoms resilience matters.
[4] Telecommunications Industry Security Advisory Council - a strategic level government group which includes senior industry representatives.
[5] European Network and Information Security Agency.
[6] http://www.niccstandards.org.uk/publications/index.cfm
[7] http://stakeholders.ofcom.org.uk/binaries/consultations/cfi-security-resilience/annexes/detica-report.pdf

2.12 DWP suggested that single points of failure have caused problems for telecoms availability in the past and should therefore be included in the guidance. As with security risks, the approach of the guidance is not to specify particular resilience improvements that should be undertaken. Such an approach would risk becoming a "design manual" for telecoms networks. The complex and fast changing nature of telecoms means that CPs are best placed to make design decisions in relation to the overall resilience of their networks and services.

Question 2 – Risk management

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?

2.13 There were some concerns expressed about the suggestion to include reference to the ENISA Technical Guideline on Security Measures[8] in our revised guidance. Several respondents stated that the standards in our original guidance were sufficient or that they did not wish to see new standards introduced. Verizon in particular were concerned this represented a change in our previous approach. These concerns seemed to result primarily from misunderstandings about the nature and role of the ENISA Guideline and whether it represents a change to our expectations of CPs.

2.14 Including a reference to the ENISA Guideline in our revised guidance does not represent a change in the range of things we would expect a CP to consider in managing general security risks, as required under section 105A(1). Neither does it suggest any change in our previous view that a CP with ISO 27001[9] certification with appropriate scope would be likely to be appropriately managing general security risks. The ENISA Guideline is not an additional or alternative standard with which we expect CPs to comply. Indeed, it is not a standard at all, but rather a checklist for regulators to consider when assessing compliance.

2.15 Six out of the seven security domains in the ENISA Guideline are drawn from ISO 27001. The only security domain which is not derived from ISO 27001, which addresses business continuity, is also likely to cover ground familiar to any CP with ISO 27001 certification.

2.16 The ENISA Guideline is therefore likely to be of most relevance to CPs without ISO 27001 or similar certification. For these CPs it provides a more comprehensive check list of the security controls that may be needed to appropriately manage risks than was included in our previous guidance. It is also more accessible than ISO 27001, and is focussed specifically on section 105A compliance.

2.17 In our previous guidance we expressed a strong preference towards CPs obtaining ND1643 certification in order to demonstrate they are compliant with the section 105A(3) obligation to protect interconnections. This position remains in the revised guidance. ND1643 includes a subset of the security controls in ISO 27001, with the scope limited to network interconnections. In the previous guidance and in discussion with CPs, we have indicated that ISO 27001 certification with appropriate scope was likely to be valid source of evidence to demonstrate that the requirements in ND1643 have been addressed. Again, we maintain this position in the revised guidance.

[8] https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures
[9] A well-established international standard addressing information security.

2.18 Sky suggested that there was "no need to go above and beyond ND1643" in demonstrating compliance. However, the obligations to manage security risks in 105A are broader than just protecting the risks to interconnections that ND1643 addresses. The limited scope of ND1643 certification does not demonstrate management of the broader range of security issues across all relevant aspects of a CP's networks and services.

2.19 EE and Three suggested our approach should be outcome based and BT suggested we should encourage CPs to adopt industry best practice. We believe that encouraging a risk-based approach based on widely accepted security best practice addresses these points.

2.20 There was general support for addressing the compliance of smaller CPs. We note that all sizes of CP are within the scope of section 105A. To date our enforcement focus has been on the largest CPs, but we will engage with smaller CPs following the publication of the revised guidance. DWP notes the need to apply the obligations proportionately to the size of CP. We agree with this point, and note that although standards like ISO 27001 are more likely to be applicable to large CPs, application of the ENISA Guideline is flexible depending on the size of a given CP.

2.21 Some CPs expressed concern about our suggestion that CPs should discuss significant new supply chain and outsourcing arrangements with us. EE and Three saw no value in pre-approval of changes in the supply chain. KCOM requested additional information, while a confidential respondent saw it as an undue burden. Vodafone said that clear principles should be set on when such engagement was expected and that we should publish the risk assessment criteria we would apply.

2.22 We note that the revised guidance does not suggest that any supply chain or outsourcing arrangements need pre-approval by Ofcom, nor is discussing plans mandatory. The range of possible supply chain and outsourcing scenarios means it is not possible to determine the risks and what might constitute "appropriate measures" to manage them in advance. Our encouragement to discuss significant new arrangements with ourselves and relevant government agencies in advance is intended to provide mutual assurance that any potential security concerns have been identified and appropriate measures undertaken.

Question 3 – Protecting end users

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

2.23 In relation to the provision of information to consumers, several respondents saw no need for intervention by Ofcom. For example, Sky stated that CPs currently have an appropriate level of flexibility in this regard and Vodafone said it should be left to the market and pointed out steps it was already taking.

2.24 Three stated that customers prefer straightforward, jargon-free advice rather than statistics. EE pointed out that placing security information in the public domain creates risk and that in their view this was not appropriate.

2.25 DWP suggested that voluntary publication of information may be a useful aid to competition, but that in practice consumers may have limited real choice.

2.26 The ICO said that while consumer transparency was welcome, providing information on a comparable basis was challenging.

2.27 KCOM said that the publication of additional information would need an agreed framework.

2.28 We continue to favour the publication of information to allow consumers to make informed purchasing decisions. We agree that ideally this would be left to CPs as part of the normal functioning of the market and accept that developing a framework to do this in a comparable way across CPs would be difficult. This is an area we will continue to consider and we welcome any further input from stakeholders.

Question 4 – Network availability

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

2.29 DWP put forward the view that there should be a legal requirement for CPs to publish availability information in real-time or near real-time. Furthermore, in its view claimed availability figures should be audited.

2.30 Most other respondents expressed a range of concerns about the publication of availability data. Several suggested that defining and capturing data comparable between CPs would be difficult. One confidential respondent said that while transparency was welcome, it required more detail on what might be published.

2.31 EE and Three suggested that consumers do not value such data, and pointed to the abandoning of previous efforts, namely TopComm and TopNet.

2.32 Sky welcomed additional information based on root-cause analysis, rather than CP performance. It suggested building on the existing information in the Infrastructure Reports.

2.33 Vodafone and a confidential respondent suggested encouraging adoption of best practice, such as business continuity standards, would be the most valuable approach.

2.34 As noted above, we continue to favour the publication of information to allow consumers to make informed purchasing decisions. However, we accept that developing meaningful availability information for comparison across CPs is difficult to achieve and may not be proportionate. We agree that more root-cause based information would be useful and we expect to expand this section of our forthcoming Infrastructure Report and provide CPs with more feedback from reporting in the future. We also note that business continuity is included in the ENISA Guideline, and we consider that this is an area which CPs need to consider in ensuring section 105A compliance.

Question 5 – Wholesale and "over the top" services

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?

2.35 BT and a confidential respondent expressed the view that only CPs with end customers should be required to report incidents. Several respondents suggested that only service providers and not network providers should be required to report. KCOM pointed out that it was difficult to include downstream customers contracted to other CPs in assessing incidents for reporting.

2.36 DWP said wholesalers should tell their customers about incidents.

2.37 Several respondents, including KCOM, EE and Three, welcomed clarity in relation to "over the top" services, but Sky said this was not necessary. Vodafone said there was no legislative basis for imposing reporting obligations relating to over the top services.

2.38 KCOM said that it saw no issue with Ofcom clarifying the need for CPs to maintain sufficient fault monitoring. However, it would be concerned if this led to an additional reporting burden beyond incidents already covered under quantitative thresholds.

2.39 In relation to network providers offering wholesale inputs to other CPs, we accept that they may have little or no visibility of the number of end users affected. We do not expect CPs to alter their network monitoring or reporting systems to obtain this information. However, where it is clear to a network provider that an incident is likely to result in service loss to end users which will exceed the reporting thresholds, we would encourage them to report this.

2.40 A CP should report qualifying incidents affecting any service it sells, even if another CP fulfils the service. However, where a CP's 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.

2.41 We understand that it is in CPs' direct commercial interest to monitor faults in their networks and services. However, for the avoidance of doubt, our revised guidance will note the need for CPs to maintain sufficient monitoring capability to meet their reporting obligations.

Question 6 – Reporting thresholds

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?

2.42 Many respondents expressed concern that lowering the existing thresholds would increase the burden of reporting and in some cases predicted significant commercial impact.

2.43 BT suggested that broadband thresholds should only be aligned with voice if voice thresholds are significantly increased. They expressed the view that these thresholds are currently too low to be of real value. They also noted that ENISA thresholds are much higher.

2.44 A confidential respondent suggested the broadband is not as important as 112/999 access and should therefore have a higher reporting threshold.

2.45 Three supported setting data thresholds in line with voice due to their increased importance. However it also made the general point that lower thresholds were not required except in relation to 112/999 and that it did not support area or infrastructure based reporting.

2.46 EE was supportive of the suggestion of area-based reporting for incidents affecting large geographic regions and large numbers of customers.

2.47 BT, the ICO and Sky all supported the suggestion of introducing relative thresholds to bring smaller CPs into the scope of reporting. However, KCOM were concerned about the burden of this approach and stated their view that current thresholds were reasonable. Vodafone suggested separate, lower, thresholds for smaller CPs to avoid excessive burden and under reporting.

2.48 Several respondents were opposed to the suggestion of reporting incidents which caused partial loss or degradation of services.

2.49 We have been very aware of the potential burden of section 105B reporting since its introduction. We have been flexible in our approach, for example in accommodating the monthly batch reporting of smaller incidents. We accept that for CPs affected by the changes we have made to the thresholds, it will take time adapt their reporting arrangements. We encourage any CPs that foresee an unduly large burden or significant commercial impact to discuss this with us.

2.50 As set out in our Call for Inputs, some of the changes to the thresholds are to reflect that the relative importance to consumers of mobile/fixed and voice/data services has changed. This means we will expect more reports from providers of mobile and broadband services. However we expect the increase in burden to be relatively small.

2.51 For mobile providers, the lowest thresholds, those for 112/999 services, already apply. In practice they are rarely triggered due to the availability of emergency roaming, and we expect this to continue to be the case. For non-999 incidents, we have not included specific quantitative thresholds as we have for fixed services. This is in response to feedback from mobile providers on the difficulty of estimating these figures for all incidents. Instead we will work with individual providers to understand which of their existing internal incident management thresholds are most appropriate.

2.52 In relation to broadband, we note that it is common for the reports we receive against voice thresholds to have also had an impact on broadband users. In many of these cases, the lowered broadband thresholds will not lead to any more reports being required. However, where incidents affect only broadband services or where only the broadband outage exceeds the thresholds, CPs will need to report where previously they would not. We feel this reflects the increased importance of broadband services, and that the thresholds we have set will ensure the additional burden is not excessive.

2.53 We note that the lowest thresholds do not relate to voice generally, but to 112/999 access. We have maintained these thresholds, as we believe even relatively small incidents can have significant impact when they affect life line access. We also note that the thresholds set by ENISA apply to national regulatory authorities for the purpose of providing annual summary reports and that they are not intended to dictate national reporting thresholds for CPs.

2.54 We have not changed our quantitative thresholds to capture partial service degradation. Quality of service is an increasingly important area, and how best to measure it is being investigated elsewhere. It may be that we need to return to this issue under section 105B in the future, as we think service degradation could fall within the meaning of "significant impact" if sufficiently severe.

Question 7 – Reporting process

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

2.55 Several respondents expressed support for flexibility in reporting, such as supporting the batch reporting of small incidents.

2.56 One confidential respondent mentioned the possibility of developing a secure portal for reporting, whereas BT and Vodafone stated a preference for e-mail. DWP suggested that reporting should be secure. Several other respondents expressed the general view that the current reporting arrangements were functioning well and did not need change.

2.57 EE and Three suggested that reporting for major incidents should occur as soon as possible or within a few hours. KCOM and Vodafone pointed out that there should be careful consideration of any rejection of non-compliant reports due to the pressures involved in submitting reports during incidents.

2.58 KCOM said it had no issue with identifying a contact point for reporting queries. BT expressed concern about a mandatory reporting template and burden this could impose. Vodafone said it would be appropriate for any change of template to be consulted upon and trialled.

2.59 The changes we have made to the reporting template are limited and we have not made its use mandatory. One field for which we have requested more specific information is location. We appreciate it is not always straightforward to provide a representative indication of location. However, it is important for us to have a reasonable understanding of the area an incident has affected, and often the information we currently receive does not allow this.

2.60 We have updated the guidance to better reflect the reporting process as it occurs in practice, such as allowing batch reporting for smaller incidents. We continue to welcome discussion with any CP about the reporting process and how the burden on it can be reduced.

2.61 In relation to the secure submission of incident reports, only one CP respondent raised this, and then only by noting that it might be an improvement. We are therefore not currently proposing to develop such a system for general use, However, we reiterate that we will endeavour to make secure reporting arrangements available for any CPs specifically requesting them.