

Cover sheet for response to BIS consultation

BASIC DETAILS <http://www.berr.gov.uk/consultations/page52743.html>

Consultation title: the new duty proposed for Ofcom to report on the UK communications infrastructure every two years.

To (BIS contact): peter.christodoulou@bis.gsi.gov.uk

Name of respondent: David Harrington

Representing (self or organisation/s): CMA

Address (if not received by email):

CONFIDENTIALITY

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

Nothing	<input checked="" type="checkbox"/>	Name/contact details/job title	<input type="checkbox"/>
Whole response	<input type="checkbox"/>	Organisation	<input type="checkbox"/>
Part of the response	<input type="checkbox"/>	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If you want part of your response, your name or your organisation not to be published, can BIS still publish a reference to the contents of your response (including, for any confidential parts, a general summary that does not disclose the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 David Harrington

Signed (if hard copy)

A Response from the Communications Management Association to the BIS consultation on the new duty proposed for Ofcom to report on the UK communications infrastructure every two years

About CMA

CMA is an association of ICT professionals from the business community who have a professional interest in communications, in both private and public sectors. It is a registered charity 50 years old, totally independent and without supplier bias. It is run by the members, for the members and aims to influence regulation and legislation, provide education and training and disseminate knowledge and information, for the public good. CMA's contribution to public consultations is generated via the process described in the Footnote to this response. (www.thecma.com)

Business Impact Statement

UKplc is now completely dependent on the global telecoms infrastructure for its global competitiveness – even its viability. Dependency may be expressed in a variety of ways, including availability, quality of service, flexibility and transparency in voice and data services riding on internet, mobile and voice communications infrastructure. We are now long past the stage where QoS might be considered a valid commercial differentiator. Business users are now reliant on the wording and integrity of SLAs/SLGs, but even this is not enough in the complexity of P2P, inter-operator agreements and outsourcing where business traffic might pass in and out of public and private networks. The ICT manager would welcome an independent assessment of what he is purchasing and what levels of assurance can be obtained from his chosen supplier. If that can be achieved UKplc can look forward to an opportunity for enhanced investment and relocation to the UK by global companies attracted by assurance of the country's telecommunications infrastructure. But without a robust approach the UK will be left on the hard shoulder of global superhighways. Cloud Computing (and the proportionately relative decline of distributed processing) is likely to massively overload our last generation networks - particularly if, in a non-resilient territory, these clouds will be over distant horizons. The resilience issue is not about the telecoms markets - it is about media, education, health, public services and what's left of the financial services industry. It is, after all, mildly myopic to look for national bragging rights for resilience when the grand aspiration for universal broadband is but 2Mb/s. The Oxford Said Business School report looks at the needs 2-3 years ahead - and resilience must be supported with symmetry, capacity and latency. We are also aware of the Commission's March 09 Communication on Critical Information Infrastructure Protection.

Summary

CMA believes that the level of dependency by UK businesses on telecommunications networks is now so great that a two-yearly assessment by Ofcom is inadequate. Once the assessment tools and protocols have been developed a case might be made for an annual review. We are, on balance, persuaded that the imposition of formal Assurance undertakings on the suppliers should be a General Condition and not a voluntary code of

practice. To that end we recommend drawing on the NISCC's resilience guide for businesses.

Discussion

We recognise that the UK is not a telecoms island and that, despite much of our MNC traffic being reliant on the frailties of foreign networks, we can control only our own telecoms environment. Even so, one has to start somewhere and this initiative provides a benchmark for other jurisdictions.

We suggest that a suitable Assurance Model should include the following inputs and methodology:

- An annual Impact Assessment by the network supplier, covering both retail and wholesale products and services;
- An annual Risk Assessment by the network supplier;
- An annual Impact Assessment by the network supplier of his critical infrastructure elements such as power supplies, water and location vulnerability;
- The provision and regular exercise of formal operational procedures covering major incident response, capability and preparedness

The above should be subject to annual, independent audit by Ofcom. Because of the non-utility nature of telecommunications, and the close relationship between these procedures and regulatory issues such as numbering, service provision and interconnection, it is not considered that other agencies such as CPNI are sufficiently empowered or have sufficient expertise to assume responsibility.

The benefits of this approach would include:

- Consistency in Service Assurance
- Proof of the UK commitment to the dependencies that companies have on the telecommunications infrastructure
- An enhanced reflection of Ofcom's primary duty of consumer protection, flowing from the improved safety and availability of the UK telecoms infrastructures.

The areas that would probably deserve particular scrutiny are:

- Points of interconnect;
- At the local edge of networks and in particular in rural areas where SMEs are more dependent on continuous service;
- All UK-wide network operators with centralised service equipment or based on regional node locations (eg: those MNOs with one exchange and thus high costs for alternative diverse links from transmitter sites to the central exchange.)

End to end resilience in any business telecoms architecture depends as much on the business's in-house plans and arrangements as it does on those of his external supplier(s). The Annex to this response contains some details on what the business user needs to do if he is to match his supplier's precautions. The NISCC's resilience guide for businesses was last updated in 2006. Ofcom might usefully review the guidelines and bring them back into mainstream use. The document can still be found here:

<http://www.cpni.gov.uk/docs/re-20040501-00393.pdf>

29 Oct 09

Footnote - CMA's Internal Consultation Process on Regulatory Issues

Any consultation document (conduc) received by or notified to CMA is analysed initially by the appropriate Forum Leader for its relevance to business users based in the UK. (The majority of CMA's members are based in this country, with a third of them having responsibility for their employers' international networks and systems).

If the document is considered to be relevant to CMA, it is passed, with initial comments, to members of both the appropriate Forum and the 20 or so members of CMA's "Regulatory College" – ie: those members who have experience in regulatory issues, either with their current employer, or previously with a supplier. The CMA Chairman is also a member of the College. The detailed comments from the College are collated by the Forum Leader in the form of a draft response to the conduc. Note: if the conduc has significant international import, the views of the international user community are likely to be sought. This is done through the International Telecoms User Group (INTUG).

Time permitting, the draft response is sent to all members of the Association, with a request for comment. Comments received are used to modify the initial draft. The final version is cleared with members of the appropriate Forum and Regulatory College (and, if the subject of the consultation is sufficiently weighty, with the CMA Board). The cleared response is sent by the CMA Secretariat to the originating authority. It might be signed off by the Leader of CMA's Regulatory Forum, and/or by the CMA Chairman.

Annex

Risk and resilience within the control of the business customer

A business user must put his own house in order before considering external risks. Such an internal exercise should take into account whether connectivity is physical, virtual or PTO routed. The main areas for internal assessment include:

- a) The assessment of risk must be based on "the single point of failure principle" for all aspects of data, internet, mobile and voice equipment including associated power supplies and within each premises of the business.
- b) Are the computers in the most important departments served from different data servers and cable driver modules?
- c) Are departments' voice ports spread over different voice system modules?
- d) Are PSTN incoming and outgoing access lines spread over different voice system modules?
- e) Can the ISP connection be easily "patched" through to a spare router and/or a different server?
- f) Has the business made any special arrangements with the ISP regarding failure of the internet connection?
- g) Are there enough mobiles in the business to justify a direct connection into/from the Main Mobile Network Operator's network?
- h) Power supplies to computers, data servers, data cable driver modules and voice systems should all have separate feeds. Consideration must be given for these essential supplies to be easily switched and powered from an emergency back-up generator.
- i) Data servers and voice system should not be located in same area of the premises.
- j) Can the data servers be located on each floor? Can the voice system modules be separated and located in different areas? Can the data and voice cables be routed in risers at each end of the premises? These are important issues and must be included in the building specification when a business considers re-locating to new premises.

It is also necessary to assess the vulnerability of elements within the "last mile" connection to a supplier's node. The risk of major disruption to all services is probably highest in this area and the business customer must have a clear understanding of his supplier's local architecture, including whether each service is a single service, or more than one, or virtual, or via outsourcing, or on a converged network, or on a hosted service.

In an outsourced contract it is important that the risk assessment decisions are included and revised after any reviews of the risks to the business.

Ideally, a minimum of two communication service access points should be available at the opposite ends of a building. It is also suggested that the business owns these access ducts and their associated access manhole points. Depending on the size of the business, the number of ducts at each building entry point needs to be agreed. Small businesses should probably aim for two ducts at each entry point. Where there are more than two suppliers a nest of four ducts is indicated. All ducts should be fitted with water and gas seals.

For a business served by a single supplier, the costs involved for alternative routing can be extremely high. Nevertheless, the most risk effective approach is to legally contract the supplier of the services to deliver such an option.