**KCOM Group PLC**

# KCOM response to the BIS consultation on proposed new duties for Ofcom on resilience

## Overview

KCOM welcomes the opportunity to comment on the proposals first aired in the Digital Britain report on this important topic. Both the Digital Britain report and the current review of the EU Telecoms framework have identified the need to ensure that telecoms networks are secure and protected against malicious and inadvertent threats. In the light of both their increasing importance to the economic well-being of the country, and mounting evidence that this is perceived as a potential opportunity to do damage by malicious forces, we agree that there is a clear need for appropriate standards setting, monitoring and enforcement powers to be put in place for the appropriate government agency. We agree that Ofcom is the right agency to undertake these responsibilities, with appropriate liaison through relevant bodies such as NICC and NGNUK.

However, in exercising such powers, it is vital that the bar is not set higher than is necessary. Whilst the consultation document does not suggest how the threshold required should be defined, and, indeed, notes that it is not the intention for Government to prescribe the level of resilience in the network, nevertheless there is a danger of “creeping scope”. In our view, this is best avoided by tying the reporting and assurance powers to those already being implemented through existing parallel activities in related areas.

## KCOM’s current commitment to resilience and network assurance

KCOM is committed to ensuring it operates a secure and resilient network to meet our customers’ reasonable service aspirations, and to fulfil our role as part of the “Critical National Infrastructure”. The notes below outline our current approach and show our commitment to achieving the goals that underpin the proposed powers.

The KCOM Network (KCN) is a sophisticated hybrid of network technologies and is designed with a strong emphasis on inherent resilience at all points of potential failure. Network resilience and disaster recovery for the KCN operates at three layers in the network architecture; physical, transport and switching. Physically diverse ducts and fibres are complemented by resilient transmission topologies and distributed switching and routing architectures for both legacy and IP service sets. Interconnects with other networks also use separate fibres and transmission protection in their design so providing inherent automatic re-routing resilience. Each of the layers has been designed with inherent resilience and every customer solution is planned and designed to ensure this high level of resilience is incorporated.

Since early September, 2009, many of the operational functions for the KCN have been contracted to BT Managed Service Limited, as part of a wide ranging network outsourcing agreement, complementing internal planning resources. These combined internal and external capabilities provide a number of ancillary services and features that complement the network and its day to day operation. These are designed to prevent failures as well as to manage the impact of any failure by utilising the inherent resilient design of the KCN, and by ensuring an effective Business Continuity process is in place across its business. This process is designed to ensure that the Company can respond in an appropriate and timely manner to events that threaten to disrupt its business activities, and to minimise any disruption to its internal and external customers.

Such services and features include:

### Network Management Centre (NMC)

KCOM has continuous real time monitoring of performance across its network. This enables immediate isolation of problems and re-routing traffic in order to minimise any likelihood of disruption to customer and network services. Monitoring of the KCN is on a 24/365 basis, with a hot standby NMC available should the master NMC become unavailable.

### Power Supply

On site dedicated DC power supply back-up is provided on all network nodes, with either permanent or mobile generator support in the event of long term power outages. This means that the KCN can operate independently of external power suppliers. Support and maintenance is provided 24/365.

### Maintenance

The network is maintained by experienced multi-disciplined engineers providing 2nd and 3rd level support, with further support available from back office technical experts. Support is provided 24/365.

### Service Level Agreements

SLAs with our switch, platform, hardware and software suppliers enable KCOM to achieve and maintain the highest of standards as a carrier class Telco network provider. The KCN performs with a network availability of greater than 99.99999% as independently audited by PriceWaterhouse Coopers.

## Business Continuity Management

The KCOM Business Continuity Management Plan (BCMP) is currently being revised to meet BS25999 standards. The BS25999 guide to Business Continuity Management (BCM) will ensure that our Business Continuity Plans (BCP) continue to identify and cover all mission critical and key risk scenarios and ensures that standard processes are used across the company.

BS25999 also ensures that a common approach is taken across KCOM when conducting Business Impact Analysis (BIA) and risk assessment. Ongoing BIA and risk assessment identifies changes to our key business process and the internal systems upon which they rely.

The business restoration strategy is being continually analysed to ensure it provides the most effective, viable and comprehensive way of restoring normality, whilst providing KCOM with a robust and proven BCM capability across all of its nationwide operations.

The plans are tested through a series of simulated failure scenarios to ensure they fully meet the recovery requirements of KCOM. All our plans and procedures are BS25999 compliant, quality checked by our Business Improvement Team, external specialist consultants and external assessment body to ensure their continued effectiveness for the future.

These plans look at the continuity of service to KCOM's customers, support services and emergency services. The current KCOM BCP is fully documented and ensures the security and resilience of our network (physical, transport and switching). Scheduled rehearsal and walkthrough exercises take into account all of the intricacies of our network to ensure that it works effectively, is flexible, viable, and can withstand the impact of an interruption to the day to day running of our business. All risks identified are analysed and prioritised and practical steps taken to minimise them.

Training programmes are in place to embed a culture of risk awareness across KCOM and ensure that all managers and staff directly responsible for the process fully understand their roles and areas of responsibility.

## EC-RRG (Electronic Communications Resilience & Response Group)

KCOM Group PLC is a full active member of the EC-RRG and is a signatory to the MOU for the provision of mutual support between CSPs (Communication Service Providers) in emergencies for planning and recovery purposes. KCOM also participates in the NEAT (National Emergency alert for Telecoms) process and the yearly EMPEX exercises to test the UK CNI (Critical National Infrastructure).

## Civil Contingencies Act

**KCOM Group PLC**

KCOM Group PLC is a Category Two responder under the terms of the Act and is a member of several unitary Emergency Planning Groups, attend LRFs (Local Resilience Forums) and participate in their exercises to test their / KCOM processes.

**Comments in response to the specific questions posed.**

## Question 1

> **Do you agree that Ofcom should have the power to require that electronic communications operators report to Ofcom on risk assessments carried out?**

KCOM accepts that the collection and reporting on risk assessments will be necessary to ensure the resilience of networks and the services that are provided over them. The key issue is whether such assessments should be within a unified framework, and, if so, what standard should be expected. Under current corporate governance practices, operational risk assessments should be the norm and, in order to meet the requirements of ISO 27001 and BS25999, these need to be both robust and comprehensive. In the first instance, KCOM believe that adherence to such standards and visibility of subsequent reports to Ofcom should be sufficient for the purposes outlined in the consultation.

However, the issues addressed in 3.1.3 and 3.1.4 are fundamental. We do have concerns about the balance between the reports required by Ofcom under this regime and the actual assessment analysis required in the reporting process. This places Ofcom as either a simple conduit or an extension of the national security agencies whose work already encompasses telecommunications CNI.

## Question 2

**Do you consider that Ofcom should have the additional power to require that further risk assessments be undertaken by relevant companies if those supplied are deemed insufficient. If so, how should this assessment process take place?**

It should be noted that Government is already addressing issues associated with security in an NGN environment, which will require or mandate suitable assurance processes for interconnection between networks and provision of services to most public sector users. In the light of the immaturity of the ”Minimum Security Standards” and the “Network Assurance” scheme, there is concern that the reporting and auditing regime required under the new proposals will represent an unwarranted step change in both complexity and cost to responsible CPs. Whilst we accept that some degree of convergence with the National Risk Assessment process may be necessary, this should not be done as an overlay but as part of an integrated regime with the existing initiatives. The emergence of “Standard Assured” products over time should address the fundamental need and the OGP has established appropriate supplier qualification processes. What does have to be clarified is how this requirement can be extended to all relevant CPs, not just those seeking to address public sector customers.

## Question 3

**Should risk assessments be based on existing Government processes?**

We would accept that any risk assessment process will not be effective if the underlying approach is not soundly based. Rather than promoting a regime where it would mandatory for Ofcom to carry out an evaluation of individual CP risk assessments, it would be better to rely upon the type of external assurance schemes noted above, which ensure that the requisite standards are met and that can also require appropriate changes to be made in order to meet the required assurance standard. This would obviate the need for any significant resource commitment by Ofcom and eliminate the possibility of “double jeopardy”.

## Question 4

**Do you agree there should be a duty on relevant companies to provide information to Ofcom on their emergency plans?**

Again, the issue of double jeopardy arises. Will the duties include consideration of regional CPNI or CCA based assessments? This exercise requires analysis of operator coverage and preparedness etc which may well duplicate activities that are already undertaken under different jurisdictions and it would clearly be unduly burdensome to require such “emergency preparedness” to be repeatedly assessed. It is clear that to enable Ofcom to report on emergency preparedness, visibility of company plans will be required – whether they do any active assessment of such plans, or accept the assessments of other agencies is the key question.

## Question 5

**Do you agree that there should be a duty on such companies to a) test emergency plans and b) participate in Government exercises as and when necessary to ensure overall resilience?**

It is reasonable to require operators providing CNI services and assured services to both test their emergency plans and participate in joint industry/Government exercises to assess overall preparedness. In our view, this approach is a much better proposition than the alternative of “regulator analysis and oversight”. We agree that testing company emergency plans is an important part of ensuring preparedness for a disruptive event – both to ensure the adequacy of the plans as well as their effectiveness, and this is a standard element of our existing BCP approach.

## Question 6

**Are there any other issues concerning the resilience of networks that you believe should be addressed in legislation?**

No

### Question 7

**Do you think that the proposals in this consultation document are in line with the expected outcome of the Framework Review?**

In general terms, yes. There is clearly a danger that, if the process of the Framework Review is extended any further, that there might be a divergence between the position eventually incorporated into the Directives proposed and that identified in the consultation. If so, this can be addressed as part of the process of Framework Implementation which may not be completed for over 18 months or so. In view of the significance of the potential problems that are being addressed, particularly as more CPs are seeking to implement NGNs, in our view it would be most appropriate to initiate change to Ofcom's powers and obligations as soon as possible.

### Question 8

**What do you think the economic impacts of these proposals will be upon your business and do you have any comments on the impact assessment?**

We note and concur with the views expressed by Alcatel-Lucent with respect to the economic assessment of costs associated with the aims identified in their "ARECI" report to the EU, that it is unlikely that commercial drivers will prove sufficient in themselves to ensure that the telecoms elements of the "critical national infrastructure" are as resilient as some would wish in all cases. It is possible that, in due course, the definition of what constitutes the telecommunications services that are fully fit for "National Emergency" and/or vital to maintaining national security interests exceeds what some or all participants are willing or able to support voluntarily to meet their commercial needs. In such cases, Government must not rule out the possible need to invest itself to ensure that all elements of the "national infrastructure" are protected at critical levels. This principle is already established in the world of "communications data retention" for equivalent national security reasons and is doubly relevant here because of the inherent mutual vulnerability of the "network of networks".

It is disappointing that the Impact Assessment glosses over this issue, in particular with regard to the "Small Firms Impact Test". It is not sufficient to characterise the UK as being dominated BT and Virginmedia as this implies that if they adhere to defined best practice that the underlying objective will be met. With interconnected IP based networks forming the core of future NGNs, vulnerabilities may be exploited on smaller networks that then cascade more generally. Clearly this does raise the prospect of proportionately higher costs being incurred by "small firms" in order to provide comprehensive security.

## Question 9

**Are there any other points you wish to make in relation to the issues covered in this consultation?**

Outages and their causes are understood to be of significant interest in the context of CPNI and their economic impact on commerce. Re-instatement of reporting of outages would be understood but needs to be in a clearly defined context. This is currently only clear in the network assured services context.