intellect
REPRESENTING THE UK TECHNOLOGY INDUSTRY

Proposed New Duties for Ofcom on resilience: Secondary Information

Intellect Response

October 2009

Russell Square House
10-12 Russell Square
London WC1B 5EE

T 020 7331 2000
F 020 7331 2040
www.intellectuk.org

Information Technology Telecommunications & Electronics Association

Contact: Henry Parker
T 020 7331 2019
E henry.parker@intellectuk.org

About Intellect

Intellect is the UK trade association for the technology industry which comprises the information and communications technologies (ICT), electronics manufacturing and design and consumer electronics (CE) sectors, including defence and space-related IT. We are formed by 780 Small to Medium Sized Enterprises (SMEs) and multinational member companies with interests in these sectors and exist solely for their benefit. Over the last 12 months, we have hosted 550 meetings attended by 3,486 people visiting our London offices and hosted 60 events for our member companies. 3,900 delegates have attended conferences we have organised in the past year. The industries that Intellect represents contribute at least 10% of the UK's GDP, employ approximately 5m people and contribute £120 billion to the UK economy.

We welcome the opportunity to comment on proposals to give Ofcom powers to require companies to report on risk assessments and emergency planning, and require them to test emergency plans and participate where necessary in Government testing of national response plans for telecommunications networks. Many of our members are significant stakeholders in the security and resilience agenda, and have been working closely with the Cabinet office and other departments on these issues for some time. A significant proportion of the design and manufacture the devices necessary for consumers to make use of electronic communications networks. Others operate telecommunications networks, and therefore directly affected by these proposals. Broadly, Intellect brings together the full range of commercial stakeholders in electronic communications networks and would ask that our standpoint be considered in the context of our views on these proposals.

Introduction

In our September 2008 paper, *A Jewel in the Crown: A national security and resilience architecture*[1], we highlighted that the UK faces a wide range of threats and hazards. They range from terrorism through to global conflict to climate change. The scale, of these challenges- and the range of stakeholders working to meet them both within and beyond Government - is significant.

The security and resilience community is fragmented- by nature and role- and coalitions are drawn together according to need. To a degree this is inevitable, as the policy areas and technologies involved are drawn from virtually every area of national life. To name but a few examples, the current 'swine flu' pandemic requires national health agencies, regional planning authorities, the Cabinet office, emergency services, and the Department for the Environment, Food and Rural Affairs (DEFRA) to come together. In the event of a significant disruption to power supply, responsibility for prioritisation of capacity, repair and recovery is shared between the National Grid, dozens of utility companies, the Department for Energy & Climate Change, and regional resilience forums, while law and order stakeholders must maintain civil stability.

Strategically, however, Intellect believes if the UK is to respond coherently to national threats this community must be able to coalesce effectively and efficiently. It is vital that all responsibility for maintaining security and resilience capability is centralised. To be clear, Intellect *do not* believe that the creation of a any new bureaucracy or database is the best way to achieve such centralisation. We continue to urge government to consider the creation of an

[1] An electronic copy of this paper can be found at www.intellectuk.org/security and is submitted as an annex to this response.

information and communications architecture that all the above named actors can use to exchange information and co-ordinate actions against a framework of responsibility that is appropriate to their direct areas of expertise. In industry's view, such a framework would offer substantial improvements in the exploitation of information, technological and human assets, and enable in future a more strategic approach to research and best practice. Creating this architecture is a technological endeavour which would improve the community's ability to co-operate. This advance in capability must be accompanied by an equivalent change in culture, which removes or lessens some of the territorial, behavioural and parochial barriers to collaboration. In order for its potential to be fully exploited, improvements in the UK's resilient, federated infrastructure must go hand in hand with improvements in these human factors. In *Jewel in the Crown,* we set out a roadmap that we believe that government, and industry, could work together in parallel to follow in order in order to construct such an architecture and move toward and elaborate on the characteristics it could have. We would urge full consideration of our proposals and analysis before moving forward with any further legislation of this nature.

It is in this context that we also urge government not to make the landscape for security and resilience policy and provision in the UK any more complicated than it needs to be. There are already multiple actors in this domain. Adding another one, ostensibly a communications regulator, and requiring it by law to take over responsibility for elements of the national resilience agenda is not the way to improve the security and resilience of UK infrastructure. In fact, it makes the co-ordination between industry and government of the resilience of critical national infrastructure more difficult. It is our understanding that those stakeholders with competence and knowledge for security and resilience planning, for example the department responsible for Critical National Infrastructure, and the Centre for Protection of National Infrastructure (administered by the Cabinet Office), are the best equipped to deal with arrangements for emergency planning by network operators and to receive information on their preparedness.

We believe that the government could facilitate greater resilience on the part of communications networks if they afforded relevant powers to existing stakeholders, and then further empowered them with a real and firm architecture for co-ordinating the huge range of actors already involved in the security and resilience agenda.

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

Intellect supports the principle that operators should supply this kind of information to Government, with the provisio that operators should all work to the same definition of what is a 'risk assessment' and, as a result, provide consistent responses. However, Intellect does not believe that Ofcom should be afforded additional powers in this area. These kinds of responsibilities are not part of Ofcom's remit in Government at present and should not become so. We firmly believe that any such responsibilities, should they be mandated should instead be housed within and actioned by the Government department responsible for the Critical National Infrastructure (CNI), in the absence of a dedicated department for national security. If Ofcom is to take on these responsibilities, they will need to work closely with operators to agree an appropriate framework for the response.

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?

As we note in our answer to Question 1), Intellect does not believe that Ofcom should be afforded any such powers. We believe that it is right and proper that companies should be required to conduct additional risk assessments of this nature. However, any such power should rest with the department responsible for Critical National Infrastructure (CNI). Furthermore, a firm structure for any reporting process, which makes it clear what is required from the outset, should be introduced along with a fully co-ordinated mechanism for exchanging information. At the outset, we would highlight that under the current proposals it appears that the details of processes that actually form additional risk assessments 'evaluations' will be determined *after* these powers have been afforded to Ofcom. There is a real need for such processes to be transparent at an early stage. Industry should not be required to go through such risk assessments repeatedly unless the outcomes are very clear from the outset. In parallel with such a process, government should also address whether the execution of a risk assessment process be sufficient, or whether they might require Ofcom to ensure that risks managed to a set standard an on an ongoing basis by network operators. We believe that if Government is to require both a risk assessment and ongoing management of risk to a certain standard, further clarity, and the agreement of industry, should be sought on those expected standards. We also believe that there is a debate to be had over how any improvements that may be required as a result of these assessments should be funded (which is discussed further in our answer to Question 5) and what the penalties are for non-compliance of these requirements might be for industry. Finally, there is a question to answer over how accurate such assessments will be. It is implicit from these proposals that any such risk assessments will be conducted internally. It will difficult to ensure consistency of approach and evaluation in these circumstances.

3) Should risk assessments be based on existing government processes?

Intellect agrees that any mandatory risk assessments should be based on existing government processes, with a number of provisios. Firstly, the assessments undertaken as part of the Civil Contingencies Act (2004) should be taken into account. There appears to be no specific reference to such assessments in these proposals. Secondly, that new legislation requiring such risk assessments is incorporated appropriately and in a timely manner, and that some form of funding is made available to industry is forthcoming, (a point we elaborate on in Question 5). These are likely to be onerous requirements for those companies deemed to be subject to them and some support is necessary. Finally, we assume that the requirement for such risk assessments will be mandatory and that relevant primary legislation contains appropriate provision for this.

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

In line with our answers to previous questions, Intellect does not believe that any such power should be afforded to Ofcom and that if industry is to be required to submit such information it should be to the department responsible for Critical National Infrastructure, which should develop the capability, in partnership with industry, to fully co-ordinate the private and public sector interests involved through an improved architecture for exchange of information. In addition, if the government does chose to implement such a requirement, we would urge that every possible measure is taken to ensure that any information on emergency plans that is supplied is not subject to the Freedom of Information Act (2000). Information of the sort that is required to confirm the availability of emergency plans and network resilience are of a commercial and competitive nature and for this reason should not be in the public domain.

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?

Intellect agrees that industry does have a responsibility to test relevant emergency plans, and to ensure that such plans can be co-ordinated with other stakeholders in partnership with Government through exercises. Such measures would ensure that overall resilience capability is maintained and improved. However, we would again highlight the need to ensure a 'level playing field'. The specific nature of the tests to be required, and the extent of the 'participation' necessary need to be clearly defined from the outset, and preferably before the powers are actually afforded to the relevant government department, and not, as we state an independent executive agency such as Ofcom. Appropriate and proportionate penalties for non-compliance need to be outlined at an early stage, as should a clear process for their enforcement. Finally, the issue of whether government should support the additional costs burden for industry as a result of such participation needs to be addressed. In particular, Intellect notes that existing legislation, in the form of the residual elements of the Telecommunications Act (1984), affords powers to government to provide such support. If industry is required to participate in exercises and conduct tests, these powers should be utilised and the costs supported by government.

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

Intellect would suggest that, in considering legislative action in this area, there is need to broaden access to the Emergency and Public Safety services network. Currently access should be consistently open, rather than being subject to a two week 'window' and a subsequent six month approval process. Access for organisations to register on the Emergency and Public Safety Services' network should be open at all times, instead the current process which sets out a two month opportunity for registration, followed by a six month approval process.

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

Intellect agrees that the expected final form of the framework review will require the UK Government to have oversight of industry input in resilience of communications networks. However, we would repeat that affording greater powers to Ofcom in this area is not the way to ensure compliance with such requirements. Delegating such powers to the department responsible for critical national infrastructure is the more appropriate mechanism for such oversight.

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

It is our firm belief, based on the experiences that existing experiences that our members have in terms of maintaining the security and resilience of their networks, that Ofcom should not have direct involvement in the security and resilience agenda in this manner. Currently, Ofcom does not have the resources in place to dispose these duties, nor the expertise to administer and adjudicate areas of the UK's critical national infrastructure. We remain available to discuss this further with the Department for Business, Innovation & Skills at their convenience.

_____END OF INTELLECT RESPONSE_____