

DIGITAL BRITAIN REPORT

Proposed New Duties for
Ofcom on resilience:
Secondary Information

SEPTEMBER 2009

PROPOSED NEW DUTIES FOR OFCOM: SECONDARY INFORMATION.....	3
1. Context.....	4
2. Explanation of Proposals	5
3. Proposals	6
3.1 Risk Assessment.....	6
3.2 Emergency Planning.....	7
3.3 Other resilience Issues	7
3.4 European Developments.....	7
3.5 Concluding Issues.....	10
4. How to respond.....	11
5. Additional Copies.....	11
6. Confidentiality & Data Protection.....	11
7 Help with Queries.....	12
Annex A - The Consultation Code of Practice Criteria	13
Annex B - List of Individuals / Organisations consulted.....	14
Annex C - Impact Assessment of Proposed new duties for Ofcom: Secondary Information...	15

PROPOSED NEW DUTIES FOR OFCOM: SECONDARY INFORMATION

This consultation seeks to identify the best way to implement the new duty proposed for Ofcom to report on the UK communications infrastructure every two years. This consultation therefore develops ideas to support the delivery of the proposed reporting objectives set out in the Digital Britain Report consultation on the proposed new duties for Ofcom published on 13 August, the scope of which includes:

- A proposed new duty on Ofcom to report to the Secretaries of State for Business, Innovation and Skills and for Culture, Media and Sport every two years giving an assessment of the UK's communications infrastructure
- A proposed requirement on Ofcom to alert those Secretaries of State to any matters of high concern regarding developments affecting the communications infrastructure

That consultation document gave examples of what the new reporting requirement might cover in terms of resilience. It suggested that Ofcom should assess mitigating actions to improve resilience and that network operators should have carried out satisfactory risk assessments on infrastructure resilience and emergency preparedness.

This consultation develops those ideas and asks what additional powers Ofcom might need to ensure that the information is available and that sufficient actions have been taken by the operators. In particular it seeks views on the propositions that:-

Ofcom should have the power to:

- a. Require companies to report to Ofcom on risk assessments and emergency planning
- b. Require companies to test emergency plans and participate where necessary in Government testing of national response plans for telecoms

The Consultation also considers how these proposals might go towards meeting the expected changes to the European Regulatory Framework that will increase requirements on national regulatory authorities and operators in regard to the security of networks.

An Impact Assessment is published at Annex C.

Issued: 15 September 2009

Respond by: 30 October 2009

Enquiries to: Peter Christodoulou
Information Economy
Department for Business, Innovation and Skills
UG 21
1 Victoria Street
LONDON
SW1H 0ET
Tel: 020 7215 6633

This consultation is relevant to: All communications network operators and those who deliver or use services carried on such networks.

1. Context

- 1.1. The Digital Britain White Paper¹ addressed the key issues that needed to be progressed to make the UK a world leader in the supply and use of digital networks and technologies. Hence, the Report acknowledged the importance of existing work on resilience and security. Indeed, there are many aspects of the current collaborative efforts of the industry to work together in times of crisis that are recognised in Digital Britain as valuable.
- 1.2. Nevertheless, the issue of resilience – the ability of any system to resist attack or failure caused by natural events or accidents and to recover from it – has risen up the national agenda as a result of both the changing national security agenda and the increased dependency on complex systems. This is particularly true of communications networks, where the nature of networks and the services that run over them has changed dramatically in the past twenty years.
- 1.3. Digital Britain therefore made recommendations on resilience and included a proposed new reporting duty to be placed on Ofcom. This reporting requirement is expressed in general terms in the Digital Britain Report: *“Ofcom should provide a full assessment of the UK communications infrastructure every two years and alert Secretaries of State to any matters of high concern regarding developments affecting the communications infrastructure”*. The consultation document issued on 13 August *“Consultation on the proposed new duties for Ofcom; to promote efficient investment in infrastructure and to provide a full assessment of UK communications infrastructure every two years”*² set out in paragraph 1.11 what this means. In terms of resilience it suggests that the report might cover:-
- An assessment of the mitigating actions to improve resilience, and, where this does not concern critical national infrastructure, emergency preparedness to ensure the availability of networks;
 - The availability of satisfactory risk assessments carried out by network operators on infrastructure resilience and emergency preparedness, including measures planned to mitigate those risks (taking into account the report of the Electronic Communications – Resilience and Response Group Chair).
- 1.4. Questions 6-8 of the 13th August consultation document seek views on the appropriate scope of the reporting requirement, and the document proposes that further consultation should take place on the specific measures that Ofcom might employ to meet the reporting requirement.
- 1.5. It is clear that the intention of these proposed resilience reporting measures is to improve, as far as possible, the delivery of communications services in the face of problems that are realistically likely to be faced.
- 1.6. For that reason, we are seeking additional comment on what powers Ofcom will need to be able to deliver the reporting requirement in terms of resilience and whether and how that role might contribute to improvements in assessment and planning.

¹ <http://www.culture.gov.uk/images/publications/digitalbritain-finalreport-jun09.pdf> - Cm 7650

² <http://www.BIS.gov.uk/consultations/page52539.html> - URN/No 09/1138

2. Explanation of Proposals

- 2.1. It is not the Government's intention to prescribe the level of resilience in the communications network, but to increase the transparency around the level of outages, the resilience and the emergency preparedness of networks. This transparency will form a basis for further policy work and allow market forces in the communications sector to take account of these factors.
- 2.2. However, the objectives of the Digital Britain project require greater assurance from network operators to the Government and the consumer that resilience will be maintained. This can best be achieved by Ofcom reporting on the basis of powers to report on what assessments of risk - and actions taken to mitigate against this - have been conducted and on whether emergency plans are in place. This tracks the likely outcome of the new European legal requirements in terms of network security (see paragraph 5.4). Information gathered in this way should be subject to strict disclosure rules. Ofcom's judgements on the state of the infrastructure should be made public but information about the security of individual companies operations will not be revealed.
- 2.3. The term 'risk assessment' will need further elaboration when the powers are exercised by Ofcom but the information which we are proposing Ofcom should be able to require companies to provide, includes data around decisions made to assess resilience, the outcome of these assessments and any further actions which are taken as a result. It also covers any commercial decisions made on what levels of risk companies are willing to accept around any issues which may affect their resilience.
- 2.4. Similarly, the term 'emergency planning' indicates the planning that takes place to ensure that companies maintain a capacity to provide incident response in the event of disruptions as well as plans to manage business and service continuity.
- 2.5. Ofcom will need to define in more detail which companies should be asked to provide this information but the intention will be to cover the key providers of the UK's communications infrastructure. In order to provide an effective assessment of overall network resilience it is important to ensure that those companies providing network services and providing very large numbers of customers with important services should be included.
- 2.6. The Government therefore proposes that Ofcom should have the power to:-
- Require companies to report to Ofcom on risk assessments and emergency planning
 - Require companies to test emergency plans and participate where necessary in Government testing of national response plans for electronic communications
- 2.7. Subject to the responses to this consultation and further consideration, the Government will consider whether legislation would be required. If so, legislation would be brought forward at the earliest opportunity.

3. Proposals

3.1. Risk Assessment

- 3.1.1. The collection and reporting on risk assessments will fulfil an important part of highlighting the work taking place to ensure the resilience of networks to ensure services are provided.
- 3.1.2. Ofcom's efforts to report on the state of UK infrastructure could be impacted by the lack of reliable risk assessments prepared by the managers of networks on the resilience of those networks.

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?

- 3.1.3. Ofcom will need to provide more information on what risk assessments a company should report on. This could be linked to the National Risk Assessment process. This annual assessment is based on some 100 scenarios that describe events that may reasonably be expected to disrupt life as normal in the UK. The events cover all facets of potential disruption from terrorist activity to natural events, such as extreme weather. From a detailed analysis of the consequences of these events Planning Assumptions are derived. When taken together the Planning Assumptions form a framework against which resilience can be assessed. This process works in close collaboration with initiatives by the Centre for the Protection of National Infrastructure focussing on critical infrastructure protection
- 3.1.4. However, the National Risk Assessment process is tailored to Government needs, and although a starting point in terms of risk assessment, is understandably not wholly suitable for companies. Ofcom will therefore need to clarify further the categories of risk assessment which will be subject to the reporting requirement.
- 3.1.5. It is not the Government's intention to mandate the level of residual risk that can be accepted but the overall assessment by Ofcom of the UK communications infrastructure, based on good quality inputs from the companies, will increase the transparency around the level of outages, and the resilience and emergency preparedness of networks.

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?

- 3.1.6. It is arguable that the risk assessment will not enable the company to adopt a suitable risk posture if it is not soundly based. To avoid this situation, it would be possible to ask Ofcom to carry out an evaluation of individual risk assessments and require changes to be made. This would require considerable resource commitment by Ofcom and expose the companies involved to regulatory uncertainty.

Question 3

Should risk assessments be based on existing Government processes?

3.2. Emergency Planning

- 3.2.1. The resilience of the networks would not be improved if the emergency plans were not fit for purpose. It is clear that to enable Ofcom to report on emergency preparedness, visibility of company plans will be required.
- 3.2.2. Again, the issue arises as to whether the existence of an emergency plan is enough to meet our objectives. It would be possible, as with risk assessments, to give Ofcom a role in assessing the worth of the emergency plan. This would be a complex activity given the differing technology, processes and organisational structures that exist in the industry.
- 3.2.3. The alternative to such analysis is for key players in this sector to test their plans and ensure that the results of the tests are part of a continuous improvement cycle. 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. There is good evidence that testing is already taking place but the reporting obligation placed on Ofcom could be said to require that there is more transparency about this activity.
- 3.2.4. In order to ensure general availability of communications services it is important to have a collaborative approach to testing industry plans and coordinating this with Government to maintain the ability to provide a coherent and rapid response in the event of wide-reaching disruptions in the system wherever possible.

Question 4

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

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?

3.3. Other resilience issues

- 3.3.1. This consultation highlights the key issues surrounding the resilience elements of the new reporting duty to be placed on Ofcom. It is, however, an opportunity to seek views on other resilience issues that might be covered in legislation.

Question 6

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

3.4. European Developments

- 3.4.1. The increased focus on the resilience of networks is reflected in other EU Member States and within the European Union. In the past two years the following major milestones have been reached:

- The Availability and Robustness of Electronic Communication Infrastructures (ARECI) study: major study and recommendations on best practice in relation to resilience (http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm),
- The development of the “European Programme for Critical Infrastructure Protection³” or EPCIP - proposals for the identification and designation of critical infrastructure that impacts on more than one country (http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/133260_en.htm)
- The Commission issued the Communication on CIIP - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm) that proposes several measures for European co-ordination to improve the resilience of networks and to test the ability of Europe to respond to a communications emergency

3.4.2. In this context, it is not surprising that the negotiations on the Revised Framework for the Regulation of Communications Services in Europe is likely to require much more from operators and regulators than previously.

3.4.3. The negotiations are currently stalled and we expect the remaining issues to be resolved in autumn 2009. The current text on network security is highly likely to survive in its current form which has been agreed by all three European institutions.

3.4.4. The text of the relevant article as it stands at the start of the conciliation stage of the negotiations is as follows:-

“SECURITY AND INTEGRITY OF NETWORKS AND SERVICES

Article 13a

Security and integrity

1. *Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services. Having regard to the state of the art, these measures shall ensure a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks.*
2. *Member States shall ensure that undertakings providing public communications networks take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks.*
3. *Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services.*

Where appropriate, the national regulatory authority concerned shall inform the national regulatory authorities in other Member States and the European Network and Information Security Agency (ENISA). The national regulatory authority concerned may inform the public or require the undertakings to do so, where it determines that disclosure of the breach is in the public interest.

³ At present, the European Programme for Critical Infrastructure Protection only covers energy and transport sectors. However, the Commission has stated its intention in the Annex to this directive that the Communications sector should be included from 2012.

Once a year, the national regulatory authority concerned shall submit a summary report to the Commission and ENISA on the notifications received and the action taken in accordance with this paragraph.

4. *The Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical implementing measures with a view to harmonising the measures referred to in paragraphs 1, 2, and 3, including measures defining the circumstances, format and procedures applicable to notification requirements. These technical implementing measures shall be based on European and international standards to the greatest extent possible, and shall not prevent Member States from adopting additional requirements in order to pursue the objectives set out in paragraphs 1 and 2.*

These implementing measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 22(3).

Article 13b

Implementation and enforcement

1. *Member States shall ensure that in order to implement Article 13a, competent national regulatory authorities have the power to issue binding instructions, including those regarding time limits for implementation, to undertakings providing public communications networks or publicly available electronic communications services.*
2. *Member States shall ensure that competent national regulatory authorities have the power to require undertakings providing public communications networks or publicly available electronic communications services to:*
 - (a) *provide information needed to assess the security and/or integrity of their services and networks, including documented security policies; and*
 - (b) *submit to a security audit carried out by a qualified independent body or a competent national authority and make the results thereof available to the national regulatory authority. The cost of the audit shall be paid by the undertaking.*
3. *Member States shall ensure that national regulatory authorities have all the powers necessary to investigate cases of non-compliance **and the effects thereof on the security and integrity of the networks.***
4. *These provisions shall be without prejudice to Article 3 of this Directive.*

3.4.5. There is clear synergy between our proposals on implementing the Digital Britain vision and what is likely to be required under the Revised Framework for the Regulation of Communications Services. Article 13a1 refers to “security” but the context does not suggest that this is security in the accepted sense of “confidentiality, integrity and availability” but rather , as indicated by the last sentence, that the focus on the improved resilience that Digital Britain requires: “to prevent and minimise the impact of security incidents on users and interconnected networks”.

3.4.6. Draft Article 13a 1 and 2 include the same requirements as the proposals set out above, that is that companies should undertake risk assessments and ensure that appropriate plans are in place to deliver continuity of supply. Article 13b1 and 2a closely mirror the proposals in this consultation document that Ofcom should be empowered to require improvements in emergency planning and should be entitled to see the risk assessment on which these response arrangements are based. Article 132(a) goes wider than the current proposals and states that the company’s “security policy” should be available to the Regulator.

3.4.7. Draft Article 13a3 also proposes that companies should be required to notify the Regulator of breaches of security or loss of integrity which has a significant impact on network operations. Moreover, the article 13b also proposes that National Regulators should have the power to investigate non-compliance with these requirements and to require companies to undergo “security audits” at their cost.

3.4.8. It is arguable that it would be premature to try and implement all of the requirements of these draft proposals. It is clear, however, that the proposals in this consultation document would be in tune with the likely outcome of the review of the Framework Directive and would give UK industry a head start in meeting these new requirements.

Question 7

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

3.5. Concluding issues

3.5.1. As part of this consultation, we would welcome information that would inform our assessment of the impact of the proposals and are keen to allow any other issues not subject to specific questions to be raised. An impact assessment is attached and we would welcome comments on it.

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?

Question 9

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

4. How to respond

When responding please state whether you are responding as an individual or representing the views of an organisation. If you are responding on behalf of an organisation, please make it clear who the organisation represents by selecting the appropriate interest group on the consultation response form and, where applicable, how the views of members were assembled.

Responses to:

Peter Christodoulou
Information Economy
Department for Business, Innovation and Skills
UG 21
1 Victoria Street
LONDON
SW1H 0ET
Tel: 020 7215 6633
e-mail: peter.christodoulou@bis.gsi.gov.uk

A list of those organisations and individuals consulted is in Annex B. We would welcome suggestions of others who may wish to be involved in this consultation process.

5. Additional Copies

You may make copies of this document without seeking permission. Further printed copies of the consultation document can be obtained from:

BIS Publications Orderline
ADMAIL 528
London SW1W 8YT
Tel: 0845-015 0010
Fax: 0845-015 0020
Minicom: 0845-015 0030
www.bis.gov.uk/publications

An electronic version can be found at www.berr.gov.uk/files/file52744.pdf

6. Confidentiality & Data Protection

Information provided in response to this consultation, including personal information, may be subject to publication or release to other parties or to disclosure in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 1998 (DPA) and the Environmental Information Regulations 2004). If you want information, including personal data that you provide, to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Department.

7. Help with queries

Questions about the policy issues raised in the document can be addressed to:

Peter Christodoulou
Information Economy
Department for Business, Innovation and Skills
UG 21
1 Victoria Street
LONDON
SW1H 0ET
Tel: 020 7215 6633
e-mail: peter.christodoulou@bis.gsi.gov.uk

A copy of the Code of Practice on Consultation is at Annex A.

Annex A: The Consultation Code of Practice Criteria

1. Formal consultation should take place at a stage when there is scope to influence policy outcome.
2. Consultation should normally last for at least 12 weeks with consideration given to longer timescales where feasible and sensible.
3. Consultation documents should be clear about the consultation process, what is being proposed, the scope to influence and the expected costs and benefits of the proposals.
4. Consultation exercise should be designed to be accessible to, and clearly targeted at, those people the exercise is intended to reach.
5. Keeping the burden of consultation to a minimum is essential if consultations are to be effective and if consultees' buy-in to the process is to be obtained.
6. Consultation responses should be analysed carefully and clear feedback should be provided to participants following the consultation.
7. Officials running consultations should seek guidance in how to run an effective consultation exercise and share what they have learned from the experience.

Comments or complaints

If you wish to comment on the conduct of this consultation or make a complaint about the way this consultation has been conducted, please write to:

Tunde Idowu,
BIS Consultation Co-ordinator,
1 Victoria Street,
London
SW1H 0ET

Telephone Tunde on 020 7215 0412
or e-mail to: Babatunde.Idowu@BIS.gsi.gov.uk

Annex B: List of Individuals/Organisations consulted

Alcatel Lucent	Microsoft
Atvod	Mayer Brown
ABFL Group – Intellex	Motorola
AOL	National Consumer Council
ACE	National Consumer Federation
BSkyB	Noonline
BSG	Nortel
BT	Nokia
BBC	Northern Ireland Office
COI	National Computing Centre
CBI	Nokia Siemens Networks
CMA	Orange
CISCO Systems	Onslow Group
Cable & Wireless	Ofcom Consumer Panel
Carphone Warehouse	Ofcom
Centre for the Protection of National Infrastructure	O2
Citizens online	Olswang
Corning inc	OFT
Cabinet Office	Political – Intellegence
Colt	Point – Topic
Childnet International	Pipex
Discovery – Europe	PCCW
Demon	Qualcomm
DCMS	RIM
DCA	Radio Regulatory Associates
Ericsson	RNIB
Eurim	RNID
EMEA	Reuters
ENPAA	Radar
Five.TV	Skype
Federation of Communications Services	Spamhaus
FCS Business Radio Group and Air – Radio	Sense
Glabal Crossing	Scottish Government
Google	Time Warner
Huawei Technologies	Telcoconsulting
Hearing Concern	T Mobile
HTA	Tiscali
Ironport	Towerhouse Consulting
Interforum	Timico
ITV	UKCTA
ISPA	UK Broadband
ICSTIS	Virgin Media
Inmarsat	Vodafone
Intellect	Verizon Business
Information Commissioners Office	Welsh Assembly
KCom	Yahoo
Merula	Z Group
Message Labs	3

Annex C: Partial Impact Assessment of Proposed new Duties for Ofcom: Secondary Information

Summary: Intervention & Options

Department /Agency:

Business, Innovation and Skills (BIS)

Title:

Impact Assessment of proposals to give Ofcom additional powers to ensure infrastructure resilience and emergency preparedness

Stage: Consultation

Version:

Date: 19th August 2009

Related Publications: Consultation on the proposed new duties for Ofcom; to promote efficient investment in infrastructure, to provide a full assessment of UK communications infrastructure every two years
<http://www.berr.gov.uk/consultations/page52539.html>

Available to view or download at:

<http://www.>

Contact for enquiries: Tim Hogan

Telephone: 020 7215 1628

What is the problem under consideration? Why is government intervention necessary?

It is crucial that the communications infrastructure is resilient as a failure to resist attack and recover quickly from it can have a potentially very significant negative impact on UK society and the economy. In preparing risk assessments and emergency plans, network operators may not take into account the impact of problems with the communications infrastructure on other businesses, consumers and citizens. As a result, their risk assessments and emergency plans may be less adequate than society would like. This provides a rationale for government intervention.

What are the policy objectives and the intended effects?

The UK Government set out in the Digital Britain White Paper its intention to ask Ofcom to provide a full assessment of the UK communications infrastructure every two years and to consider what the report might cover in terms of resilience. This could include an assessment of the mitigating actions taken by network operators to improve resilience and the availability of satisfactory risk assessments carried out by network operators on infrastructure resilience and emergency preparedness.

The UK Government is now seeking to identify the best way to implement the new powers being proposed for Ofcom and asking whether Ofcom might need further powers to ensure that the relevant information is available and that sufficient actions have been taken by the network operators

What policy options have been considered? Please justify any preferred option.

Option 1: Do nothing

Option 2: Grant Ofcom additional powers to:

- a) Require companies to provide information to Ofcom on risk assessments and emergency plans
- b) Require companies to test emergency plans and participate where necessary in Government testing of national response plans for telecoms

When will the policy be reviewed to establish the actual costs and benefits and the achievement of the desired effects? An updated impact assessment containing a more detailed discussion of the costs and benefits will be published later in the year.

Ministerial Sign-off For consultation stage Impact Assessments:

I have read the Impact Assessment and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options.

Signed by the responsible Minister:

.....Date:

Summary: Analysis & Evidence

Policy Option:	Description:
-----------------------	---------------------

COSTS	ANNUAL COSTS	Description and scale of key monetised costs by 'main affected groups' Potential increase in administrative burdens for some network operators if they are required to submit extra information about risk assessments and emergency plans and further costs associated with testing them. Ofcom may also incur further resource costs associated with gathering and collating the additional material they receive
	One-off (Transition) Yrs	
	£	
	Average Annual Cost (excluding one-off)	
£	Total Cost (PV)	£
Other key non-monetised costs by 'main affected groups'		

BENEFITS	ANNUAL BENEFITS	Description and scale of key monetised benefits by 'main affected groups'
	One-off Yrs	
	£	
	Average Annual Benefit (excluding one-off)	
£	Total Benefit (PV)	£
Other key non-monetised benefits by 'main affected groups' Main identifiable benefit would be any further improvement in the delivery of communications services in the event of problems that are realistically likely to be faced – potentially mitigating the disruption to economic activity and the daily lives of consumers and citizens		

Key Assumptions/Sensitivities/Risks

Price Base Year	Time Period Years	Net Benefit Range (NPV) £	NET BENEFIT (NPV Best estimate) £
--------------------	----------------------	-------------------------------------	---

What is the geographic coverage of the policy/option?	UK
On what date will the policy be implemented?	
Which organisation(s) will enforce the policy?	Ofcom
What is the total annual cost of enforcement for these organisations?	£
Does enforcement comply with Hampton principles?	Yes
Will implementation go beyond minimum EU requirements?	N/A
What is the value of the proposed offsetting measure per year?	£
What is the value of changes in greenhouse gas emissions?	£
Will the proposal have a significant impact on competition?	Yes/No
Annual cost (£-£) per organisation (excluding one-off)	Micro Small Medium Large
Are any of these organisations exempt?	Yes/No Yes/No N/A N/A

Impact on Admin Burdens Baseline (2005 Prices)		(Increase - Decrease)
Increase of £	Decrease of £	Net Impact £

Key: Annual costs and benefits: Constant Prices (Net) Present Value

Background

The issue of resilience – the ability of any system to resist attack and to recover from it – has risen up the national agenda as a result of both the changing national security agenda and the increased dependency on complex systems. This is particularly true of communications networks, where the nature of networks and the services that run over them has changed dramatically in the past twenty years.

In the Digital Britain White Paper the UK Government set out its intention to ask Ofcom to provide a full assessment of the UK communications infrastructure every two years and alert the Secretaries of State to any matters of high concern regarding developments affecting the communications infrastructure. Provision for this intention was included in the Government's Draft Legislative Programme, published alongside Building Britain's Future⁴.

The subsequent consultation document "*Consultation on the proposed new duties for Ofcom; to promote efficient investment in infrastructure, to provide a full assessment of UK communications infrastructure every two years*"⁵ sets out what the report might cover in terms of resilience:

- An assessment of the mitigating actions to improve resilience, and, where this does not concern critical national infrastructure, emergency preparedness to ensure the availability of networks;
- The availability of satisfactory risk assessments carried out by network operators on infrastructure resilience and emergency preparedness, including measures planned to mitigate those risks (taking into account the report of the Electronic Communications Resilience and Response Group Chair).

The UK Government is now seeking to identify the best way to implement the new powers being proposed for Ofcom and in its latest consultation document "*Proposed new duties for Ofcom: secondary information*" is asking what additional powers Ofcom might need to ensure that the relevant information is available and that sufficient actions have been taken by the network operators.

Rationale for Government Intervention

Communications infrastructure – be it for example fixed or mobile telephony or broadband – underpins all economic activity and social and cultural way of life in the UK. It is therefore crucial that the communications infrastructure is sufficiently resilient as a failure to resist attack and recover quickly from it can have a potentially very significant negative impact on UK society and the economy. There are several reasons for this:

⁴ <http://www.hmg.gov.uk/buildingbritainsfuture.aspx> Cm 7654

⁵ BIS (2009) *Consultation on the proposed new duties for Ofcom; to promote efficient investment in infrastructure and to provide a full assessment of UK communications infrastructure every two years*
<http://www.berr.gov.uk/consultations/page52539.html>

Large number of users of communications

Nearly every individual and business is connected to each other via one communications platform or another, and uptake continues to increase. Consequently, any problem with the communications infrastructure or the ability of the market to function efficiently has the potential to affect a very large number of people.

The ICT sector is of major economic importance to the UK economy

The information and communication technology (ICT) sector is of major economic importance, forming the backbone of the UK economy. In 2007, it generated some £96 billion in gross value added and employed some 1.2 million people. This represents around 8% of total UK GDP and 4% of total UK employment⁶. ICT is also a powerful driver of productivity and innovation and thus makes a positive contribution to the competitiveness of a large number of sectors many of which the UK enjoys a significant comparative advantage (e.g. business services, financial services, computer and IT services and the content and creative industries).

Emergency services

A high speed and reliable communications infrastructure is crucial to the delivery of emergency services. A failure to contact the emergency services promptly because of problems with the communications infrastructure can contribute to a loss of life as people in urgent need of medical attention do not receive it in time.

Delivery of public services

Greater certainty of well functioning communications infrastructure also has an important role to play in helping the UK Government achieve equity objectives such as greater social inclusion and the provision of high quality public services in more rural and remote areas of the country. The existence of technical problems with the infrastructure may hamper the ability of the UK Government to achieve these goals.

Wider strategic importance

Communications makes a significant contribution to the wider infrastructure and strategic interests of the UK. For example, radar, broadband and Global Positioning Systems (GPS) all play a vital role in air traffic control and military and defence systems.

⁶ See page 4 of the impact assessment produced alongside the Digital Britain Final Report which can be accessed at: http://www.culture.gov.uk/images/publications/digitalbritain_impactassessment.pdf

In preparing risk assessments and emergency plans, network operators may not take into account the impact of problems with the communications infrastructure on other businesses, consumers and citizens. As a result, their risk assessments and emergency plans may be less adequate than society would like. This provides a rationale for government intervention.

Policy options

Option 1: Do nothing

Under this option, Ofcom would continue to assess infrastructure resilience and emergency preparedness on the basis of information currently supplied by network operators. This could serve to limit further increases in transparency around the level of outages, resilience and the emergency preparedness of networks and accordingly potentially limit any further possible improvements in the delivery of communication services in the face of problems associated with the infrastructure.

Option 2: Grant Ofcom additional powers

Under this option, Ofcom would be given additional powers to:

- a) Require companies to provide information to Ofcom on risk assessments and emergency plans
- b) Require companies to test emergency plans and participate where necessary in Government testing of national response plans for telecoms

Costs

Administrative burdens for some network operators may increase if, as a result of these proposals, they are required to provide Ofcom with new additional information on risk assessments and emergency plans which they previously did not use to submit. It is also possible that network operators may incur further costs associated with testing emergency plans and participating where necessary in Government testing of national response plans for telecoms. Ofcom may incur additional resource costs associated with gathering and collating the additional information which they receive from network operators. All of these various costs have not been quantified at this time.

Benefits

The main identifiable benefit would be any further improvement in the delivery of communications services in the event of problems that are realistically likely to be faced, potentially mitigating the disruption to economic activity and the daily lives of consumers and citizens.

Competition Assessment

After initial screening, it has been deemed that these proposals would not have a significant impact on competition. It is unlikely to directly or indirectly limit the number of network operators and internet service providers, limit their ability to compete or the incentives to do so.

Small Firms Impact Test

The communications infrastructure in the UK is dominated by the two main network operators, BT and Virgin Media. It is possible that there may be an impact on the smaller network operators who may incur disproportionately higher costs associated with carrying out satisfactory risk assessments and improving their emergency plans if they are judged to be inadequate by Ofcom.

Other specific tests

Other specific tests have been considered including Legal Aid, Sustainable Development, Carbon Assessment, Other Environment, Health Impact Assessment, Race Equality, Disability Equality, Gender Equality, Human Rights and Rural Proofing.

After an initial screening, it has been deemed that no significant impact is anticipated in any case. Nevertheless, a more detailed analysis would be presented in an updated impact assessment which would be published alongside any legislative proposals.

Specific Impact Tests: Checklist

Use the table below to demonstrate how broadly you have considered the potential impacts of your policy options.

Ensure that the results of any tests that impact on the cost-benefit analysis are contained within the main evidence base; other results may be annexed.

Type of testing undertaken	<i>Results in Evidence Base?</i>	<i>Results annexed?</i>
Competition Assessment	Yes	No
Small Firms Impact Test	Yes	No
Legal Aid	No	No
Sustainable Development	No	No
Carbon Assessment	No	No
Other Environment	No	No
Health Impact Assessment	No	No
Race Equality	No	No
Disability Equality	No	No
Gender Equality	No	No
Human Rights	No	No
Rural Proofing	No	No