Impact of Security and Integrity provisions of the EU Electronic Communications Framework

A Detica report commissioned by the Department for Culture, Media and Sport

April 2011

CVCA1181D001
Copy 1
Cover + 59 pages

List of contents

List of Tables and Figures

List of Tables

List of Figures

INTENTIONALLY BLANK

1 Executive Summary

1 Executive Summary

This report seeks to develop the evidence base underpinning the Government's implementation of new security and integrity provisions within the revised European Union Electronic Communications Framework. In particular it aims to answer the following questions:

- What measures do UK communication providers currently take to ensure the security and integrity of their electronic communication networks and services? How much do they spend on these measures?
- What are the additional costs to communication providers and the National Regulatory Authority of the amended Framework Directive?

Given the short project timelines, the approach taken in this work was to conduct one-to-one interviews with senior security managers from 23 communication providers (providers of fixed voice, broadband and mobile networks and services) to ascertain an indicative baseline for current spending by communication service providers on security and integrity of their electronic communication networks and services.

As the approach is based on extrapolating the costs from a small number of communication service providers compared to the sector as a whole, there are clear limitations in that firms may differ in compliance. Hence there are significant uncertainties around these results and they should be treated as indicative estimates rather than accurate and robust estimates.

Given that the Government's approach is to copy the text of the security and integrity provision of the Directive into new stand alone provisions in the Communications Act 2003, potential scenarios for implementing the new security and integrity provisions of the amended Framework Directive needed to be identified in cooperation with the Department for Culture, Media and Sport, and Ofcom. A gap analysis was then performed against these potential scenarios.

It is likely that the implementation of the new provisions will complement and reinforce existing legislation, regulation and information exchanges such as those reporting requirements arising from the Digital Economy Act 2010, and the forums in place under the remit of the Centre for the Protection of National Infrastructure.

The status of broadcasters within the above definition of ECF is unconfirmed. Broadcasters have been included within this assessment for completeness and since they are within scope for the DEA; however it is not anticipated that implementation of Article 13 will ultimately encompass broadcasters or broadcast network providers.

The report finds that overall, providers are fulfilling the basic requirements of security and integrity. In particular, appropriate measures are implemented covering the majority of the key control areas and their selection is based to some extent upon risk management decisions.

1 Executive Summary

The acceptable risks to a provider are driven by the commercial requirements for service availability and network security. Frequently this means the use of service level agreements for suppliers or wholesale customers, or customer satisfaction indices for retail customers. Therefore a key area for potential improvement within the sector is compliance with specific technical standards where appropriate.

The report suggests that the current operational expenditure for risk, security and incident management is in the order of £200m per year for telecoms providers. This is in addition to the initial and ongoing investment in the networks, and their operational support systems, to provide an inherent level of redundancy and resilience.

The Government's preferred approach is for light-touch regulation. Therefore the additional impact of the security and integrity provisions is expected to be modest – arising primarily from the investigatory powers of Ofcom rather than any requirement to implement additional technical or operational measures.

As a result it is estimated that Ofcom, as the National Regulatory Authority, could incur ongoing operational costs in the region of £250k per annum, while providers could incur ongoing operational costs in the region of £220k per annum.

However, if more enhanced regulations – the medium scenario considered in this report – are implemented, in particular the mandating of any particular standards across the market, then the impact is likely to be far greater with small providers disproportionately effected. In particular small providers could incur costs of up to £18.5m in the first year, with considerable ongoing operational costs thereafter. Table 1-1 summarises the direct cost impact on Ofcom and the CSPs.

1 Executive Summary

Article	Anticipated Degree of Regulation	Cost impact on Ofcom	Direct cost impact on CSPs	Benefits and other comments
13a(1)	Low or Medium	None	Application of Medium requirements to all (small) CSPs could cost £6m per annum	Improved and harmonised risk management across the sector
13a(2)	Low or Medium	None	Application of Medium requirements to all (small) CSPs could cost £12.5m in first year with additional operating costs in following years	Improved security of interconnecting networks, allowing for greater assurance between CSPs Reduction of significant outages, resulting in a more reliable service for the customer
13a(3)	Medium	£50,000 per annum	Negligible	Improve awareness of and response to significant incidents Concerns over commercial confidentiality and reputational image
13a(4)	N/A	None	None	-
13b	Medium	£145,000 per annum	£220,000 per annum	-
Background resource	N/A	£55,000 per annum	None	-
Total	N/A	£250,000 per annum	At Low - £220,000 per annum At Medium - £12.5m in first year, in excess of £6.22m thereafter	-

Table 1-1: Summary potential impact of security and integrity provisions of the Electronic Communications Directives

2 Introduction

2 Introduction

2.1 Background to the report

Information and Communications Technology (ICT) is a key enabler in the UK economy. Businesses rely on ICT to operate efficiently and to access a wide customer base. Consumers rely on e-communication in their daily activities; more than 90 per cent of households have a mobile telephone and almost three quarters have an Internet connection[1]. A high speed and reliable communications infrastructure is also critical to the functioning of Government and the delivery of emergency services.

The security and integrity of telecommunications is an issue of increasing national and international prominence. This is driven by increased dependency on complex communication systems, as well as a changing national security agenda. Telecommunications networks possess high levels of inherent integrity and generally have good levels of in-built security.

However, there remain significant concerns where network and information security are at risk, whether from deliberate or accidental disruption. One in three of UK companies suffered an incident of loss of IT in 2010 while one in five suffered a loss of telecommunications (Ref [20]). The causes of such outages vary from equipment theft or damage, environmental threats such as flooding, and electronic network attacks such as Denial of Service attacks; for more details see Section 3.3.

The European Electronic Communications Framework (ECF)

In 2002, EU Member States reached agreement on a regulatory framework, the Electronic Communications Framework, for electronic communication networks and services. The framework encompasses telecommunications (fixed and mobile), email, access to the Internet and content-related broadcasting. Its aim was to harmonise regulation governing the provision of e-communications across the EU, to help:

- reduce entry barriers;
- foster effective competition;
- lead to the creation of an internal market sector.

The ECF included provisions for review and consequently the Commission proposed changes in November 2007. The revised Framework was agreed in November 2009 and must be implemented by the UK and other Member States by 25 May 2011.

[1] Based on figures at http://media.ofcom.org.uk/facts/.

2 Introduction

Consultation process

The Government published a consultation paper on implementing the revised EU framework in September 2010. The official Government response will be published in April 2011. DCMS has lead responsibility for ensuring the necessary legislative and policy changes are implemented by 25 May 2011[2].

Ofcom will then work in conjunction with industry to develop the processes necessary for the implementation to work in practice.

Article 13 – 'Security and integrity of networks and services'

The amended Framework Directive, 2002/21/EC (Ref [9]), introduces new provisions on security and integrity – Articles 13a and 13b. These place obligations on public electronic communications network and service providers to take appropriate steps to ensure the security and integrity of public networks and services. It also defines a new role for the National Regulatory Authority (NRA) – Ofcom in the UK – in terms of monitoring and enforcement (see Appendix A.1 for definitions).

The Government's preferred option for implementing the provisions on security and integrity is to copy out the text in the ECF into new standalone provisions in the Communications Act 2003 (Ref [5]).

A number of the provisions set out in the legislation already represent UK industry practice to some extent, and in some cases are duplicated by existing regulatory requirements arising from the Digital Economy Act 2010 (DEA) (Ref [7]). These include the selection of security measures and notification to relevant authorities. Article 13 formalises these processes and allows for a coherent reporting and enforcement structure to be built on them. However, it is expected that the resulting regulations will result in additional operational and capital expenditure both for communications providers and Ofcom. In the main these costs will be driven by specific regulatory decisions, such as the setting of minimum standards to which the sector must adhere. Such decisions have not yet been taken.

The new requirements pertaining to security and integrity can broadly be summarised as:

- Implementation of "appropriate technical and organisational measures" along with risk management procedures to determine these,
- Notification of breach to Ofcom and the European Network and Information Security Agency (ENISA),

[2] In December 2010, The Prime Minister decided that competition issues relating to the media, broadcasting, digital and telecoms sectors would transfer from the Department for Business, Innovation and Skills (BIS) to the Department for Culture, Media and Sport (DCMS). The machinery of government change has since taken place and responsibility has been transferred for these areas, which includes telecoms policy and the implementation of the EU framework. The Department for Business, Innovation & Skills retains responsibility for security and resilience.

- Powers vested in Ofcom for investigation, request for information, commissioning of audit and issuance of binding instructions.

2.2 Objectives of the assessment

The core objective of this report is to develop the evidence base to support the final stage Impact Assessment that will accompany the Government response and the laying of the regulations in Parliament.

The consultation-stage Impact Assessment which accompanied the paper on proposals for implementation (Ref [2]) was entirely qualitative in nature. A quantitative analysis of the economic impacts was not possible at that time because the practical implementation of the Directive had not been agreed. None the less, that analysis identified, for the majority of the costs, the nature of those costs and where they would fall.

The study has two elements:

The first element establishes a baseline for the current level of spending in the UK on security and integrity for electronic communication networks and services, providing insights into the measures that providers take. Essentially, it attempts to answer the questions:

- What measures do UK communication providers currently take to ensure the security and integrity of their electronic communication networks and services?
- How much do they spend on these measures?

The second element seeks to analyse, and where possible quantify, the direct costs of the security provisions in the revised EU Directive on providers. It attempts to answer the question:

- What are the additional costs to communication providers and Ofcom of the security and integrity provisions of the amended Framework Directive?

It must be emphasised at this point that the objective of this report is to consider only the direct costs of the Directive and is not intended to perform detailed analysis of indirect costs or of the benefits to the telecommunications sector and to the wider economy.

2.3 Methodology

Information capture

The approach taken in this work was to conduct one-to-one interviews with senior security managers from 23 Communications Service Providers (CSPs). Given the tight project timeframe, the survey sample had to be kept relatively small, compared to the total number of CSPs which has been estimated to be in the region of 600. The CSPs interviewed were selected following consultation with the Government and Ofcom in order to provide a representative sample across the different service offerings (fixed/mobile, voice/data, consumer/corporate) and include those that specifically responded to the public consultation.

Each interview examined the CSPs' approach to each of the following areas:

- information security risk management;
- quality of service / availability;
- standards and compliance;
- supplier management;
- incident management;
- security spending.

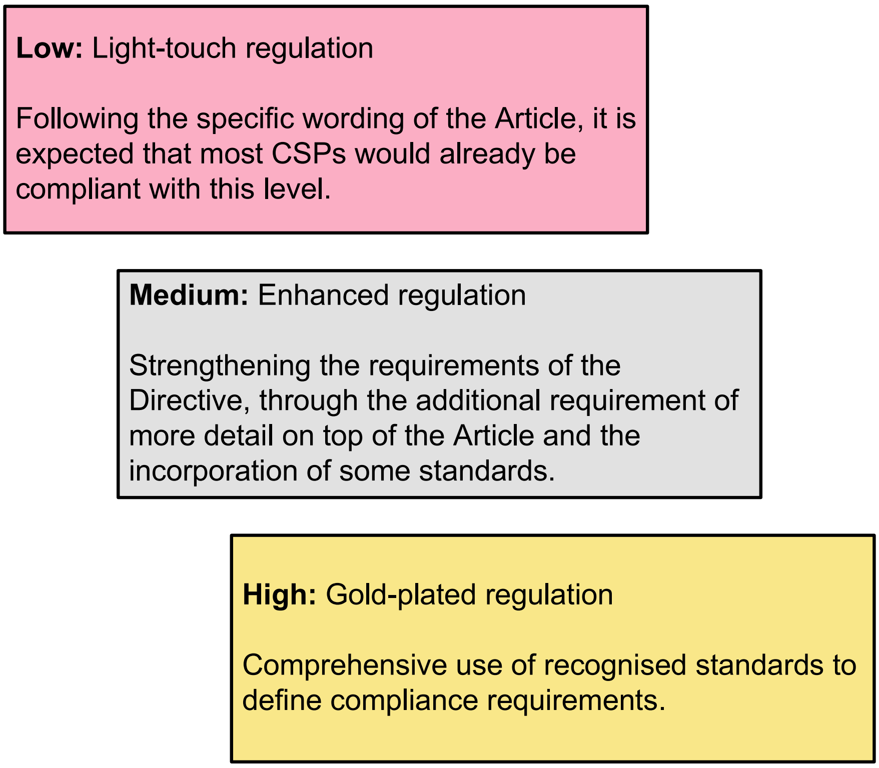
Where possible certain technical aspects, such as physical security, power supply integrity and redundancy of data centres and data centre equipment were also covered. The above method allowed the current baseline level of compliance, and where possible spending, to be identified.

The list of questions used within the interviews is provided for reference within Appendix A.4.

Implementation scenarios

Since the regulations that arise from the ECF are yet to be defined, the second part of the work required the definition of a number of scenarios for implementation of each of the provisions of the ECF. These have been defined, in dialogue with DCMS and Ofcom, according to three levels of regulation, as shown in Figure 2-1.

These scenarios have been depicted in a necessarily stylised manner in order to facilitate analysis, and it should be recognised that there is a continuum of possible scenarios for implementation. This means some CSPs will face greater or lesser costs than those estimated, and Government and Ofcom will need to use appropriate judgement in setting the various thresholds in practice. We provide more detail of the scenarios for each part of the article in the relevant sections.



Low: Light-touch regulation

Following the specific wording of the Article, it is expected that most CSPs would already be compliant with this level.

Medium: Enhanced regulation

Strengthening the requirements of the Directive, through the additional requirement of more detail on top of the Article and the incorporation of some standards.

High: Gold-plated regulation

Comprehensive use of recognised standards to define compliance requirements.

Figure 2-1: Degrees of regulation

Ascertaining the current Baseline and the additional impacts

For Article 13a, the next stage of the work was a gap analysis of the CSPs' current baseline against the scenarios defined. For this purpose the CSPs were grouped into three broad categories (see Section 2.4). There does remain some variation of compliance within each category at a detailed level, but it is felt that this grouping represents a sufficient degree of granularity and adequately allows for the analysis to be performed. In addition, the data has been aggregated to ensure that individual organisations, and their current state of security management, cannot be identified, to ensure the confidentiality of their responses.

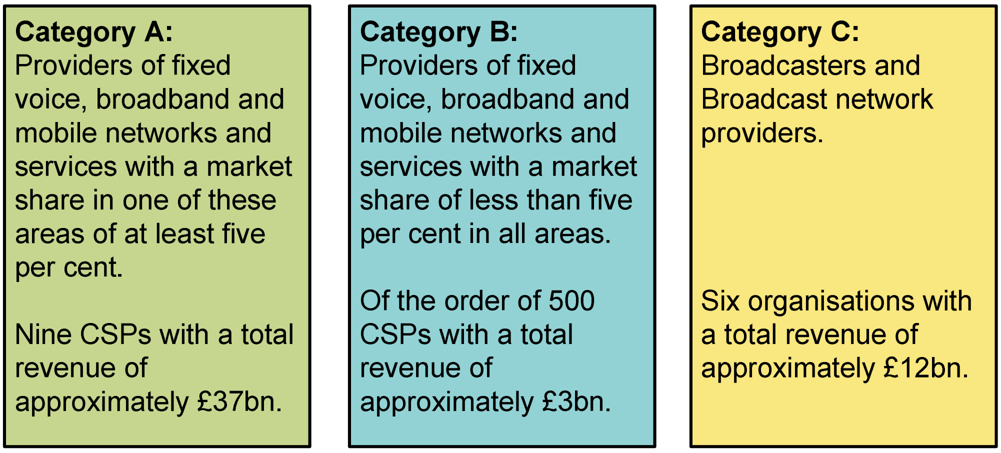
The report itself then quantifies the impact, within each CSP category, of implementing the Low, Medium and High scenarios. The inputs to this assessment were based upon information gathered within the interview stage, industry baselines and specialised knowledge of the necessary requirements for meeting particular standards – from these a standard cost for each organisation was identified which was then extrapolated across the size of the market for each Category. Costs were calculated either as an increase of a proportion of revenue or as a fixed amount per organisation and are expected to differ for each Category of CSP reflecting their differing nature.

We have attempted to quantify direct cost implications of the possible implementation scenarios. However, we have not quantified, or assessed in any depth, the potential returns on investment arising from implementation. For example, the cost incurred to certify compliance against a standard such as ISO27001 (Ref [12]) or BS25999 (Ref [3]) could be recovered from elevated revenue arising from increased confidence among prospective customers or simply reduced operating costs from fewer incidents that are of shorter duration and less expensive to remedy.

For Article 13b the approach was slightly different since the impact does not depend on CSPs current processes and procedures, but rather on the scale of implementation by Ofcom. Here the key inputs were discussions with DCMS and Ofcom as well as using industry knowledge of how these provisions will impact on the CSPs.

2.4 Overview of stakeholders

As mentioned in Section 2.3, for the purposes of this work the CSPs have been categorised into three groups as shown in Figure 2-2:



Category A:
Providers of fixed voice, broadband and mobile networks and services with a market share in one of these areas of at least five per cent.

Nine CSPs with a total revenue of approximately £37bn.

Category B:
Providers of fixed voice, broadband and mobile networks and services with a market share of less than five per cent in all areas.

Of the order of 500 CSPs with a total revenue of approximately £3bn.

Category C:
Broadcasters and Broadcast network providers.

Six organisations with a total revenue of approximately £12bn.

Figure 2-2: Categories of CSP (Revenue estimates derived from Ref [16])

It should be noted that the 17 CSPs identified within Annex 7 of the DEA Infrastructure Report (Ref [7])[3] are distributed across all three of these categories.[4]

The status of broadcasters within the above definition of ECF is unconfirmed. Broadcasters have been included within this assessment for completeness and since they are within scope for the DEA; however it is not anticipated that implementation of Article 13 will ultimately encompass broadcasters or broadcast network providers.

[3] Under the DEA Ofcom are required to produce an Infrastructure Report every three years that provides an accurate picture of the state of the country's communications infrastructure.

[4] It should be noted that these Categories of CSP are in no way intended to align to Category 1 and Category 2 responders defined in the Civil Contingencies Act 2004.

As noted above, the methodology adopted in this work was to obtain a representative sample from each of these categories. In total 23 CSPs and Industry Bodies were invited to take part in this work with 13 providing a comprehensive response. The responses were freely given by the CSPs in an open manner providing all the information requested where it was possible within the timescale. The 23 stakeholders represented (based on figures at http://media.ofcom.org.uk/facts/):

- 11 of the 17 CSPs identified in Annex 7 of Infrastructure Report;
- CSPs with over 60 per cent of all fixed broadband subscribers[5];
- CSPs with over 40 per cent of all mobile phone subscribers;
- CSPs with over 65 per cent of all fixed telephone line subscribers.

The 23 stakeholders was formed from seven Category A, twelve Category B and two Category C CSPs along with two industry bodies.

2.4.1 Strengths and weaknesses of the approach

Due to the timescales for performing the research it was not possible to make contact with any great number of the many smaller providers. Therefore there are more assumptions and greater extrapolation across companies for each sector of the market than would be ideal. The key assumptions are that the basis of the impact calculations are representative across the sector being considered. These are detailed within each section of the research findings.

As the approach is based on extrapolating the costs from a small number of interviews to the sector as a whole, there are clear limitations in that firms may differ in compliance. Hence there are significant uncertainties around these results and they should be treated as indicative estimates rather than accurate and robust estimates.

On the positive side, the research does provide coverage of the majority of subscribers and so provides confidence of the impact on most CSPs from a customer perspective.

Further it has not been possible to obtain exact values of spend on risk management or on security controls themselves. For this reason the potential impacts identified should be viewed as an indicative estimate of the broad nature of the impacts rather than accurate and robust estimates.

[5] The proportions covered by this report of market share by revenue are of a similar order. Detailed revenue proportions can be found in http://stakeholders.ofcom.org.uk/binaries/research/cmr/Q4_2010.pdf

2.5 Document structure

This report is structured in the following manner:

- *Chapter 3: Scope and Context of Articles* – confirms the scope of Article 13 and discusses various aspects of how the provisions relate to existing legislation and regulations.
- *Chapter 4*: *Research Findings* – describes the measurement of the baseline for current spending, and compliance against the potential scenarios for implementation of Article 13, and provides the assessment of the additional impacts from those scenarios.
- *Chapter 5: Conclusions* – summarises the research findings and provides an overall assessment of the security and integrity provisions of the revised EU electronic communications framework.
- *Appendix* – provides definitions, references, glossary and interview questions.

INTENTIONALLY BLANK

3 Scope and Context of Articles

3 Scope and Context of Articles

3.1 Scope

As set out in the ECF and the Communications Act 2003 (Ref [5]), we maintain the distinction between a Public Electronic Communications Network (PECN) and a Publicly Available Electronic Communications Service (PAECS), the definitions of which are given in Appendix A.1 for completeness.

Our scope includes both fixed and mobile network operators providing voice, data and IP broadband services. This includes Internet Service Providers (ISPs) and Mobile Virtual Network Operators (MVNOs).

The status of broadcasters within the above definition of ECF is unconfirmed. As noted above, broadcasters have been included within this assessment for completeness and since they are within scope for the DEA; however it is not anticipated that implementation of Article 13 will ultimately encompass broadcasters or broadcast network providers.

We expressly exclude public sector networks such as the Government Secure Intranet (GSi) and Airwave, and private Critical National Infrastructure (CNI) networks such as BACSTEL-IP®. These are not considered to be publicly accessible in a direct sense and their security risks are generally well understood and managed by the relevant parties.

3.2 Context and general remarks

This section is intended to place Article 13a and 13b within the context of existing legislation, regulation and other activities.

Intent of ECF

The primary intent of the “Security and Integrity” provisions is to drive improvement in the availability of communications networks and encourage pan-European harmonisation of measures taken to safeguard such availability through a common regulatory framework.

A further expectation is that the provisions will improve the transparency of security and reliability of the PAECS to the customer, potentially enabling a greater understanding of the availability levels of a service at the point of purchase.

It should be noted that there are many other elements to the ECF. This includes the ePrivacy Directive (2002/58/EC, Ref [10]) which in particular requires notification of breach of security of personal data. For this reason, discussion of breaches of this type are explicitly out of scope of this report.

Existing drivers for security

The security of PECN and PAECS has thus far been driven entirely by commercial requirements. These typically take the form of contractual Service Level Agreements (SLAs) with suppliers or with wholesale or business customers. In the retail sector they take the form of internal customer satisfaction measures and retention targets.

As such, while there are various technical standards relating to the security of networks (see *Relevant standards* below), the industry is currently free to implement whichever measures it deems appropriate to meet its commercial requirements. This is particularly the case for the smaller CSPs that need to be more agile and responsive to be competitive.

Relevant standards

There are a number of national and international standards that concern information security and integrity; some apply to all sectors and some are specific to the telecommunications sector:

- ISO/IEC 27001 (Ref [12]) is an international standard that defines an information security management system (ISMS) providing a framework for security risk management within an organisation. It can be applied to any organisation and it is possible to obtain certification against the standard. It does not stipulate any specific technical measures.
- ISO/IEC 27002 (Ref [13]) complements the ISO27001 standard by listing a control set comprising 133 technical, procedural, personnel and physical controls that can be selected to manage risk, and includes implementation guidance on each. It is not possible to certify against this standard.
- BS25999 (Ref [3]) is a British standard that defines a business continuity management system. It can be applied to any organisation and it is possible to obtain certification against the standard.
- ISO/IEC 27011 (Ref [14], and also known as X.1051) is an international standard that builds upon and extends the ISO/IEC 27002 control set aimed at the telecommunication industry. It tailors guidance to the telecommunications providers and adds 12 new controls specific to the sector, including guidance on security in co-location situations.
- ND1643 (Ref [17]) is a 23-control subset of ISO/IEC 27002 tailored to telecommunication interconnects. It aims to represent a minimum standard required to protect the UK national telecommunications infrastructure. The key areas of control are: general security and incident management, physical security, logging and auditing, control of data flows across interconnects, and vulnerability management.

- The CESG Security Procedures – Telecommunications Systems and Services (Ref [4]) is a security standard for operating telecommunications networks to the "2-2-4" Impact Levels. This refers to the CESG Business Impact Levels for Confidentiality, Integrity and Availability respectively. It mandates ISO27001 compliance and stipulates specific details of the compliance such as a minimum scope and minimum threat assessment. It also presents a control set drawn from ISO/IEC 27002 and 27011, but actually mandates the implementation of most (107) of them. 32 remain optional (intended to be driven by risk assessment). It is possible to obtain certification against this standard.

Digital Economy Act 2010 Infrastructure Report

The Digital Economy Act 2010 (DEA) (Ref [7]) already gives Ofcom a number of new duties, including a duty to report on the UK's communications infrastructure on a three-year basis (the first is due in 2011). The Infrastructure Report (Ref [8]) is designed to:

> "Provide Government, industry and consumers with a clear indication of the state of the health of the communications infrastructure."

In particular there are two components of the Infrastructure Report that have considerable duplication with Article 13a, namely those of Availability and Resilience:

- Availability: It is proposed that two types of incident should be reported:
  - major outages, requiring details of impact, cause and actions taken;
  - minor outages, requiring statistical data on service availability levels.
- Resilience: It is proposed that those CSPs within scope report summaries of risk assessments and emergency planning, mitigation measures, implementation plans, accepted risks and standards compliance.

Mechanisms for information exchange

Despite a lack of regulation in this area, there exist mechanisms for information exchange between the larger CSPs that have arisen from collaborative working. These include:

- The Centre for the Protection of National Infrastructure (CPNI) UK Network Security Information Exchange (UK-NSIE). This forum meets under a strict information sharing protocol to share sensitive information in the information and telecommunications sector. It enables discussions that include threats to communications networks and mitigation measures implemented. Participating companies represent 80 per cent of the telecommunications market in the UK. Details can be found at:

  http://www.cpni.gov.uk/Products/information.aspx.

- The Electronic Communications Resilience and Response Group (EC-RRG) develops and shares best practice in improving resilience and coordinates responses to emergencies that occur. Details can be found at:

  http://interim.cabinetoffice.gov.uk/ukresilience/preparedness/ccact/cat2_info/telecoms.aspx.

- The National Emergency Alert for Telecommunications (NEAT) is a protocol for sharing information among members of the EC-RRG. NEAT is triggered in the event of circumstances that may effect the operation of telecommunications networks. Specific aspects of the protocol are tested annual through exercises. Details can be found at:

  http://interim.cabinetoffice.gov.uk/ukresilience/preparedness/ccact/cat2_info/telecoms.aspx.

It is important to note that participation in each of the above is voluntary for most CSPs. The UK-NSIE is a proactive and pre-emptive collaboration, whereas NEAT is a reactionary process. The EC-RRG is proactive from the perspective of facilitating NEAT exercises to test and maintain its effectiveness.

The need for Government intervention

Market failures can occur in instances where free and competitive markets do not lead to an efficient outcome from a societal point of view. In the telecommunications sector there are two prevailing features, identified below, that may prevent economically efficient decisions being made with regards to security and integrity. In order to remedy this outcome, well designed government interventions may be required.

In the electronic communications sector there are two prevailing features that may prevent economically efficient decisions being made from a societal point of view, with regards to security and resilience. In order to remedy this outcome, well designed government interventions may be required.

Public good – security and resilience of communications infrastructure could be considered to have the characteristics of a public good, like emergency services. It is non rival – consumption of the good does not reduce availability for others and non excludable – no one can be excluded from consuming the good.

Externalities – during the past two decades the number of communication providers and their coverage has increased significantly, as well as the services provided across them and customer usage of these. In order to function, these networks need to interconnect. Therefore, a security threat to one network has a direct impact on others, making it crucial that all networks maintain a certain level of resilience.

Furthermore, any threats to network security and resilience may have an impact on the vast majority of UK households and businesses that are reliant on communications, be it fixed/ mobile telephony or broadband. Individual firms equate private costs with private benefits, and they will not factor in the potential cost of a network breakdown on the UK economy as a whole.

3.3 Scale of the issue

The UK communications networks and services face a number of threats and incidents do occur on a regular basis. The purpose of this section is to provide a summary of the nature of network incidents that occur and the common threats to which networks are exposed.

Incidents broadly fall into the three tiers which are used in this report (figures for frequency and impact are based upon information gathered during this research):

- Faults – These are high frequency, low impact incidents. These occur relatively regularly (on the order of 1000s per month), but the effect may be negligible or only impact a small group of customers (typically 50 to 2000). Faults may be resolved before customers notice a problem, but in some cases may last several hours and be reported in the local press. A common cause is cable damage or theft.
- Significant Incidents – These are incidents likely to impact, or threaten to impact, of the order of 10,000 customers or more, and/or are likely to effect multiple CSPs. Information gathered through this work suggests that they occur on the order of 20 per month and are often referred to internally by organisations as “major” incidents. It is estimated that approximately a quarter are due to network failures and the rest service failures. Two recent examples are described below, under *Environment threats*.
- Major Incidents – These are extended outages or network failures (lasting 24 to 48 hours or more) requiring major redirections and typically effecting entire regions (note that the distinction between Significant and Major Incidents is not a ‘hard’ threshold and is likely to be determined in each case). Those that are publicly reported in the press occur roughly twice per year, but it is anticipated that they may be up to 10 a year. A key example is a telecoms tunnel fire in 2004. Electrical maintenance works were blamed for causing a fire in a tunnel under Manchester city centre that cut off 130,000 phone lines in the area, damaged the emergency services radio network, and closed up to 30 bank branches for several days. Mobile phone networks were also reported to be disrupted.

Cable theft

The price of copper rose by 30 per cent in 2010, and entered 2011 at a record high (see http://www.bbc.co.uk/news/business-12098576). Strong industrial output in emerging economies such as China, India and Brazil, as well as the impact of industrial disputes and natural disasters on supply, has seen demand outstrip supply.

The surge in the value of this metal is having a significant impact on communication network providers. Traditional telephone circuits comprise pairs of copper cable, and thieves are increasingly targeting these in an attempt to sell the copper for scrap. This has led to a large number of localised outages across the UK. Networks relying on copper are not the only ones at risk. Fibre optic cables are regularly targeted and damaged by copper thieves unaware of the nature of the cables.

The scale of cable theft is difficult to assess, since most organisations do not record, let alone disclose, the full extent or impact of the problem. The impact of any one theft can be significant:

- In March 2010 the broadband and TV services of around 17,000 customers in Leeds were disrupted by thieves cutting through fibre to reach a copper cable (see http://www.guardian.co.uk/leeds/2010/mar/23/virgin-media-down-in-leeds).
- In April 2010 copper cables were stolen in Kent, denying over 2,000 people with landline telephone and broadband services (see http://news.bbc.co.uk/1/hi/england/kent/8642871.stm).

Cable damage

Cables are also frequently damaged by accident. Construction work is a major contributor, with diggers frequently responsible for severed cables. Another cause is damage caused by maintenance works to utilities supplies.

A major vulnerability in the cabling infrastructure is its complex development over the decades. Due to the high costs and disruptive effects of street works, it has been commonplace for network providers to install cables in ducts owned by water and gas companies when these companies are carrying out their own maintenance. Attempts to develop inventories of this infrastructure to support risk assessment have usually met with insurmountable complexities and incomplete information.

Environmental threats

Equipment damage at exchanges caused by local environmental incidents has been known to cause major disruption in the past. In both March/April and December of 2010, local flooding caused electrical fires at communications exchanges that led to wide-spread outages effecting tens of thousands of customers, with the impact being felt in areas of the country distant from the effected exchange itself. Other fixed and mobile CSPs frequently observed knock-on disruption and in some cases disruption has also been reported within the card payment systems in the area.

Human Error

Given the considerable work involved in maintaining a telecoms networks there is always the potential for human error to cause an outage, particular where work is being performed on core network elements. There are a number of procedural controls that reduce the likelihood of this occurring, for instance a full configuration and change management process, training for engineering and maintenance staff, and restricting and segregating logical access as far as possible.

Major national events

Major national events can pose a significant threat to the provision of telecommunications services. These events can impact on telecommunications networks in a number of different, though generally indirect ways.

The 2005 London Bombings did not damage physical infrastructure, but networks were quickly overwhelmed by the volume of traffic in the aftermath. The floods in 2007 caused wide-spread disruption to power supplies which in turn required CSPs continuity plans to be enacted. The three fuel crises of the last decade have meant some operators have been unable to carry out timely maintenance and repairs during those periods as CSPs are not defined as having an emergency requirement for fuel.

Denial of Service attacks

Denial of Service (DoS) attacks attempt to effect disruption by flooding networks and services with excessive traffic in an attempt to overwhelm them. These attacks often take the form of “Distributed” sources of DoS traffic (termed DDoS), and these days usually originate from networks of infected PCs known as botnets.

Typically DoS and DDoS attacks target websites. However, in 2002 and again in 2007 a subset of the main Internet root servers came under attack in an attempt to disrupt the Internet backbone. In both cases the disruption appears to have been minimal, and lessons learned in the 2002 attack informed better mitigation ahead of the 2007 one.

Motivations behind DoS attacks vary, and sometimes remain unclear. Often they are politically motivated, such as the attacks on Estonia in 2007, the attacks on Georgia during the 2008 South Ossetia crisis, and the attacks on the US and South Korea in 2009. Most recently in 2011, the Tunisian and Egyptian governments have been targeted during the ongoing periods of unrest.

A recent trend is the rise of a cyber protest phenomenon known as “hacktivism”. This is often ideologically motivated. At the end of 2010 during the US Diplomatic Cables leak by WikiLeaks, a disparate group of supporters launched DDoS attacks against companies that were seen to be withdrawing resources from the organisation. In this case widely available software was modified to allow sympathetic users to contribute their computers to a botnet carrying out the DDoS attacks.

ID Theft

It is widely recognised that one of the major areas of risk presented by the internet is that of identify theft. In particular there is believed to be a considerable economic impact, on the individual as well as on businesses.

While identity theft is frequently committed using mechanisms such as DoS and malicious software propagated across telecoms networks, it is primarily aimed at the end-point content providers (ie website themselves) rather than at the network elements. This issue is considered to be more relevant to the ePrivacy Directive (Ref [10]) and so has not been considered within this research.

INTENTIONALLY BLANK

4 Research Findings

4 Research Findings

4.1 Structure of chapter

This chapter presents the findings of the research for each of the sub-Articles of the Directive in turn.

Each sub-section follows the same format:

- The wording of the Article is provided along with any key interpretative statements.
- The three potential scenarios for implementation are presented, with relevant discussion.
- The indicative baseline for current spending for each of the Categories of CSP against these three scenarios is presented, with a summary table, along with quantitative estimates of current expenditure where possible.
- The additional impact (direct cost) of implementing each of these scenarios is then presented, with a summary table.

4.2 Risk management

> **Article 13a(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.

As noted within the Consultation (Ref [1]) this Article is understood to imply that differing networks and services will require differing measures according to risk-based identification of appropriateness to the network or service in question.

4.2.1 Possible scenarios for implementation

Degree of regulation	Description
Low	CSPs are requested to evidence that risk management procedures are in place in compliance with the wording of Article 13a(1). Ofcom would request such evidence on an individual basis wherever there is believed to be an issue of non-compliance.
Medium	CSPs are requested to evidence that robust risk management procedures are in place, that are integrated with enterprise risk management frameworks, and/or are assessed to be formed of the elements described in Sections 4-10 of ISO27001. CSPs should ensure appropriate input is provided by relevant bodies such as CPNI and EC-RRG. Ofcom would request such evidence on an individual basis wherever there is believed to be an issue of non-compliance.
High	CSPs are requested to evidence strict compliance with or Certification to ISO27001 on a regular (annual) basis.

Table 4-1: Implementation scenarios for Article 13a(1)

As previously mentioned in Section 3.2, there is significant duplication with the Resilience section of the DEA Infrastructure Report (Ref [8]), which requires the larger CSPs to provide information about their risk management practices, including outputs of risk assessments and risk treatment plans. The level of detail required suggests that those CSPs for whom the report is applicable will necessarily have in place structured and robust information security management systems and so are likely to be required to meet the Medium level of regulation already.

It should also be noted that the relevance and effectiveness of an ISO27001 Certification is entirely dependent on the defined scope for the Certificate. Therefore, were the High degree of regulation implemented there would need to be serious consideration of the required scope of Certifications.

4.2.2 Current baseline

All organisations that responded had some form of risk management within the organisation. The strength of this risk management is usually in proportion to the size of the organisation.

Through the information gathering element of this work Category A CSPs have been assessed as, in all known cases, meeting the Medium degree of regulation, and in many cases have relevant and existing ISO27001 Certifications. In addition, these organisations have a variety of mechanisms for ensuring consistency of risk consideration, for instance through involvement in the CPNI's NSIE.

For the Category B CSPs there is much greater diversity in the maturity of risk management. The smallest CSPs do not have specific Information Security Management Systems but may consider security type risks on an informal basis at system design stage, or in general terms through light weight corporate risk management. There are Category B CSPs who have gone right through to ISO27001 Certification, and this is often as a result of commercial requirements.

Category C CSPs have been assessed as meeting the Medium degree of regulation, in particular they invariably have risk management frameworks that are integrated with the business to ensure appropriate acceptance of risk and may have performed internal compliance assessments against ISO27001.

The assessed levels of compliance for each of the CSP categories against the three implementation scenarios is shown in Table 4-2, where the blue bars signify the effective levels of compliance of CSPs within each category:

Category of CSP	No risk management	Low	Medium	High	Baseline spend
A			🟦	🟦	£185m
B		🟦	🟦	🟦	£9m
C			🟦		Not available

Table 4-2: Current baseline assessment of CSPs' compliance for Article 13a(1)

Through discussions with CSPs it has been possible to obtain an indicative baseline for information security spend for those organisations where defined security roles exist. This is based upon operational costs for resourcing security functions, including risk management, incident management, business continuity management, policy and strategy and technical security operations. The resulting baseline broadly matches the indicative figures provided within industry surveys, including the PWC Information Security Breaches Survey 2010 (Ref [18]).

The indicative figure is that 0.5 per cent of an organisation's total revenue is spent on information security. This is consistent with approximately 5 per cent of total revenues being spent on IT (within technology and telecoms companies), and 10 per cent of IT budget being spent on security (Ref [18]).

Therefore for Category A CSPs as a whole it is estimated that of the order of **£185m**[6] is spent on security.

While this formula holds for the larger Category B CSPs (where a formal security management system is generally in place), the more numerous smaller CSPs (accounting for approximately half of the Category B revenue) are expected to have a much lower proportional spend of 0.1 per cent, in particular due to the lack of dedicated security functions. As a result, for Category B CSPs as a whole it is estimated that in the region of **£9m**[7] is spent on security.

Due to the nature of the small number of providers within Category C and the limited timescale of this report, it has not been to accurately determine the current baseline spend on risk management within this sector.

4.2.3 Additional impact of new provisions

Impact at Low or Medium scenarios

Given the established baseline, were the regulations to be broadly at the level of the Low or Medium scenarios, there would be negligible impact on Category A, Category C and the larger Category B CSPs. In effect, the Resilience element of the DEA Infrastructure Report (Ref [8]) already requires an ability to provide evidence of robust security risk management.

The requirement to have a robust security risk management system will hit hardest within the many smaller CSPs. If the direct cost impact is estimated by increasing the proportional spend on security to rise to 0.5 per cent in line with other organisations then the impact would be an annual increase in costs of **£6m**[8] for the Category as a whole – a not inconsiderable 66 per cent increase on the current spending estimate of £9m for Category B CSPs. This is felt to be a conservative estimate.

[6] This is based upon 0.5% of £37bn total revenue for the category

[7] This is based upon 0.5% of half of the £3bn total revenue for the category, and 0.1% of the other half

[8] This is based upon an increase from 0.1% to 0.5% for half of the total revenue of the category

While the degree of regulation may remain light-touch at these levels, extra benefits may be obtained by ensuring that all parties are able to effectively exchange methodologies, risk profiles, mitigation measures and good practices through forums such as the EC-RRG or the NSIE. This will require some strengthening of these forums but will ensure consistency across all providers and improve risk mitigation measures.

Impact at High scenario

The mandating of certification with ISO27001 would be a significant step above the current baseline for all Categories of CSP. While the risk management frameworks that exist will, for all but the smallest CSPs, be largely compliant there is a considerable administrative burden to collate and maintain evidence of compliance and to fulfil the regular independent audits.

For each Category A and C CSP the direct financial impact of such a requirement is estimated to be formed of 1 FTE (at £50k per annum per CSP) to initially collate, and then maintain, evidence and ensure all elements are in place; and annual audit/certification body requirements (approximately £10k per CSP). Due to certifications already in place around half of Category A and most of Category C would require certification: at a cost of up to **£600k**[9] per annum.

For Category B CSPs, the impact would be far greater, while resource requirements may be more of the order of 0.5 FTE and audits will be smaller scale (approximately £5k per CSP), the large number of small organisations would result in costs of up to **£15m**[10] per annum in this sector on top of the additional £6m impact identified as a result of the medium scenario.

For Category A CSPs, this extra expenditure, while significant, is relatively small compared to current levels of spend. However the increased expenditure for Category B CSPs has the potential to impact on the profitability of smaller companies, constituting 0.5% of the total revenue of these CSPs.

Clearly there are commercial benefits to obtaining certification and in many cases, while not quantified here, this would cover and potentially exceed the costs incurred.

Category of CSP	Low	Medium	High
A	Negligible	Negligible	£240k per annum
B	Negligible	£6m per annum	£15m per annum
C	Negligible	Negligible	£360k per annum
Ofcom	Negligible	Negligible	Negligible

Table 4-3: Summary cost of regulation of Article 13a(1) per Category of CSP

[9] This is formed of £60k per CSP for a total of 10 CSPs

[10] This is based upon an additional 0.5% of £3bn total revenue for this category

4.3 Guarantee of integrity

> **Article 13a(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.

There are a number of vital points to note regarding the proposed interpretation of this provision:

- it explicitly relates to network providers only and not to service providers;
- the Government interprets the word “integrity” to represent the information security industry’s concept of “availability”, which is frequently referred to as resilience in the case of electronic networks;
- the Government notes that it is “impossible to provide such a guarantee, as under hostile conditions networks will fail regardless of the steps taken to protect them” (Ref [1]);
- it is also noted in the DCMS consultation that what is “appropriate” will be explicitly driven by service level offerings and legitimate customer expectations and is assumed to be implicitly informed by identified risks.

4.3.1 Possible scenarios for implementation

Degree of regulation	Description
Low	CSPs are requested to evidence that appropriate measures have been implemented to meet relevant commercial requirements (for instance contractual SLAs). Ofcom would request such evidence on an individual basis wherever there is believed to be an issue of non-compliance.
Medium	CSPs are mandated to be compliant with the Minimum Security Standard for Interconnecting Providers (NICC ND1643) (Ref [17]). Ofcom would require proactive confirmation of compliance/certification.
High	CSPs are mandated to be compliant with CESG Security Procedures – Telecommunications Systems and Services (Ref [4]). Ofcom would require proactive confirmation of compliance/certification.

Table 4-4: Implementation scenarios of Article 13a(2)

It should be noted that the DEA Infrastructure Report (Ref [8]) requires a statement of whether the CSP is compliant with ND1643 or any of the ISO270xx family – it does not however mandate such compliance nor any formal certification.

4.3.2 Current baseline

Across all categories of CSP the fundamental driver for implementation of security controls is to meet whatever commercial requirements exist for the network or service in question. In the vast majority of cases, for PECNs, this takes the form of customer satisfaction (for retail) or contractual SLAs (for wholesale).

In certain cases, in particular for Category A CSPs, the commercial drivers themselves require compliance with certain standards, namely ND1643 or CESG Security Procedures – Telecommunications Systems and Services, and in those cases the CSP has obtained, or is in the process of obtaining, appropriate certification. In some cases, informal internal assessments of compliance with ND1643 have been completed in the expectation that this will become a requirement in the near future.

The scope of this report does not include assessing CSPs against any particular standard however, certain areas of control were explored where possible. All indications were that, even where an internal assessment has not been made, the key elements of ND1643 are being considered and implemented by the majority of Category A and Category B CSPs.

However, a key point to be noted again is that SME organisations (ie the smaller CSPs within Category B) have a specific business model to be highly flexible and agile in order to provide a competitive service. As such there is a distinct aversion to aligning with any particular technical standard unless there is a clear commercial benefit in doing so.

There is a concern within the industry that the mandating of any particular standard may be counter-productive. Firstly, the strength of the standard would likely be either too low, and so not useful, or too high, and so impractical. Secondly, the commercial value of achieving a particular standard would be undermined were that standard mandated to all providers in the sector.

Finally for Category C CSPs, the referenced technical standards are not currently seen as relevant at this time. Again, the limited explorations made within this work did not highlight any considerable areas of weakness but a full assessment of such is outside the scope of this report.

The assessed levels of compliance for each of the CSP categories against the three implementation scenarios is shown in Table 4-5:

Category of CSP	No measures	Low	Medium	High	Baseline spend
A			🟦	🟦	Not available
B		🟦	🟦		Not available
C		🟦			Not available

Table 4-5: Current baseline assessment of CSPs' compliance for Article 13a(2)

It has not been possible to identify the capital expenditure required to implement the current level of security within the PECNs. This is because such expenditure is an intrinsic part of the network build, while there is considerable investment in legacy and new networks to ensure redundancy, resilience and security, separate security or resilience funding streams not identified by CSPs and so can not be identified within this research. It can be expected that the investment in technical security and integrity measures may reach into the £bns as a portion of the general expenditure by CSPs on their networks.

4.3.3 Additional impact of new provisions

Impact at Low or Medium scenarios

For Category A CSPs, the mandating of ND1643 is unlikely to have a significant impact; all parties questioned had completed internal assessment against this standard (or higher) and determined that their networks and services were compliant. There may be a small overhead to ensure evidence is in place to allow an external audit, but this is considered negligible as invariably there exist Governance or Compliance functions within these organisations that perform this work already.

For Category B CSPs the capital cost of compliance with an ND1643-type standard would be small, though probably not insignificant, as the exploratory analysis performed within this work suggests that the key controls were being considered by all parties. However there would be a far increased cost of initial and ongoing evidencing and certifying compliance. Such work would require the equivalent of 0.5 FTE at each of the CSPs. This would therefore total **£12.5m**[11] for the Category as whole.

The group of Category C CSPs is relatively small and currently there is no particular standard that directly relates to the infrastructure concerned. Therefore an assessment of the additional impact of standardisation has not been made, though it is suggested that Ofcom work directly with the individual suppliers to understand the risks and mitigations in place.

In view of the threats described in Section 3.3, the provisions of Article 13a(2) have a clear place in protecting the UK telecommunications infrastructure. While measures to protect resilience will usually be driven by market forces, it is reasonable to insist on specific control measures where it is necessary to protect network interconnects. A risk that is acceptable to one party will not always be acceptable to an interconnect partner, and therefore it is beneficial to introduce powers that enable this risk to be managed in a coordinated manner.

[11] This is based upon £25k costs per CSP across of the order of 500 CSPs

Impact at High scenario

The mandating of a more stringent standard, such as the CESG Telecommunications Systems and Services standard[12], would however place a considerable extra burden upon those CSPs that have not assessed compliance, with many additional technical and procedural controls being required. The exact cost of meeting such a standard is likely to vary considerably according to the extent to which such controls are already in place. Some indications are that the initial implementation of a standard may as much as double a CSP's spend on security in the year of implementation; in addition there are would be significant ongoing costs to maintain such a standard.

Given that only a small proportion of Category A CSPs do not currently have compliance with the CESG standard it is therefore estimated that mandating this standard would cost **£20m**[13] in the initial year. Mandating compliance to Category B CSPs would similarly require a large one-off doubling current security spending of **£15m**[14] in the first year.

Category of CSP	Low	Medium	High
A	Negligible	Negligible	£20m capital
B	Negligible	£12.5m capital	£15m capital
C	Negligible	Not applicable	Not applicable
Ofcom	Negligible	Negligible	Negligible

Table 4-6: Summary cost of regulation of Article 13a(2) per Category of CSP

[12] It should be noted that this standard is being used here for illustrative purposes and is unlikely to be relevant to all CSPs.

[13] This is based upon approximately 10% of the sector by revenue requiring certification – the current security spend of this group therefore being approximately 10% of £185m

[14] This is based upon all CSPs in the category requiring certification, with £15m being security spend once risk management is in place

4.4 Notification of breach

Article 13a(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.

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.

The Government anticipates that notification to other Member States or ENISA would likely be exercised only were an incident to impact outside of the UK.

It is also expected that "public interest" will apply in situations such as when it would allow customers to take some mitigating action that would otherwise not be available to them. In any case strong justification would be required. It should be noted, however, that in the UK Ofcom will be subject to Freedom of Information requests from the public and media.

Ofcom will need to establish a working arrangement with the Information Commissioner's Office to avoid duplication of effort where there is a potential crossover with data protection notification requirements.

4.4.1 Possible scenarios for implementation

The different implementation scenarios for Article 13a(3) relate to the possible interpretations of "significant", and the levels of detail required:

Degree of regulation	Description
Low	A light implementation would see the threshold for significance set quite high, with only Major Incidents reported. It would also require manual notification to Ofcom, which would operate an informal management system to handle the notifications.
Medium	At the middle of the scale a medium threshold would be set, requiring the reporting of Significant Incidents in addition to Major Incidents. Notification would still be manual but regular, and Ofcom would operate a formal process for keeping records.
High	At the highest end of the scale the threshold for significance would be low, with the reporting of any faults that cause a failure to meet SLA availability targets or impact on availability for even a small group of customers. Notification would be automatic, most likely integrated with provider's real-time monitoring systems. Ofcom would operate a sophisticated management and analysis system.

Table 4-7: Implementation scenarios of Article 13a(3)

It should be noted that some incidents, in particular Significant and Major Incidents, will lead to multiple reports to Ofcom as they will effect more than one CSP (either through supply chains or by the scale and breadth of outage).

It should also be noted that the Medium threshold would be commensurate with the DEA Infrastructure Report (Ref [8]) section on major outages. However that report asks CSPs to look retrospectively at their top incidents over a three month period preceding the Infrastructure Report's next collation, whereas the requirements for Article 13a(3) would be for proactive notification at the time of the outage.

Further, the High implementation (reporting on even minor outages) is more in line with the DEA Infrastructure Report (Ref [8]) section on availability performance figures.

4.4.2 Current baseline

Most PECN providers use real-time, or near real-time monitoring of their infrastructure to detect faults and malicious traffic, and have mature incident management processes for categorising incidents, prioritising responses, investigating causes and recording the events. In addition, all Category A CSPs, and the larger Category B CSPs participate within NEAT and EC-RRG during multi-CSP incidents and exercises.

Category B providers are more varied but are still medium to high on the implementation scale. Commercial pressures typically drive a need to monitor performance against SLA targets, but formal incident management could be strengthened. In addition, there is a lack of involvement of the smaller parties to the relevant forums for incident response.

In some cases CSPs are effectively reliant on suppliers where they have procured a managed service, incident response is in some cases therefore very light weight while still meeting the Medium requirements due to the suppliers procedures.

Category C CSPs all maintain a High baseline for monitoring and notification. In particular, multiplex operators already provide Ofcom with detailed availability information as part of their licence requirements.

The assessed levels of compliance for each of the CSP categories against the three implementation scenarios is shown in Table 4-8:

Category of CSP	No incident management	Low	Medium	High	Baseline spend
A			🟦	🟦	Not applicable
B			🟦	🟦	Not applicable
C				🟦	Not applicable

Table 4-8: Current baseline assessment of CSPs' compliance for Article 13a(3)

At present there is no NRA that requires notifications of breach by CSPs. Therefore the analysis of current baseline is not relevant.

4.4.3 Additional impact of new provisions

Impact at Low or Medium scenarios

Due to the current baseline in all parts of the stakeholder community, the implementation of Low or Medium scenarios are not expected to result in any significant impact to the CSPs.

The existing processes involving NEAT and EC-RRG are in place to respond to Significant and Major incidents, and it would simply require Ofcom to be made aware of, and provided with details of, any such incident. As noted above, there may be a requirement to strengthen the effectiveness of these forums; in particular smaller CSPs should be given an opportunity to be involved even if they do no attend on mass.

Given the anticipated number of Significant and Major Incidents, Ofcom will require a small resource to manage and response to such incidents. This has been estimated by Ofcom as equivalent to **£43k**[15] per annum, though would depend significantly upon the number of incidents reported and the depth of investigation into each.

[15] Ofcom have estimated that the monitoring activities will require a minimum annual resource of 0.2 FTE at Principal level and 0.8 FTE at Associate level, which equates to a total cost over one year of £43k.

A further, indirect, impact of the requirement to notify is that of a breach of commercial confidentiality or conflict with other legislation such as the Data Protection Act (Ref [6]) or the Regulation of Investigatory Powers Act (Ref [19]). This may be directly through Ofcom notifications to the public, or through Freedom of Information (Ref [11]) requests received, to which Ofcom is open while CSPs and CPNI are not. The resultant impact on reputation and goodwill cannot be quantified but is of considerable value to the CSPs. Therefore consideration should be made of the content of notifications, and of how this information is handled and disclosed.

In contrast, there are expected to be clear benefits from greater transparency within and outside the sector to network service levels and availability. Firstly, lessons learnt by one CSP can and should be shared across the sector to enable all parties to make relevant improvements. Secondly, transparency of availability levels to the customer will make quality of service a far greater factor of choice, leading to improved service levels through open competition.

Impact at High scenario

The High scenario defines a low threshold for reporting of incidents. As such it requires far more automated processes and would provide more statistical data more akin to the general availability levels required within the DEA Infrastructure Report (Ref [8]).

As stated above, most PECNs perform continual network monitoring for their own commercial purposes. However, making full Quality of Service data available to Ofcom will require a common standard for determining such data along with potentially considerable research, development and investment in new technology by parts of the sector to meet the requirement in full. Such investment may total **£10m**[16] over a number of years.

For the smaller Category B CSPs, complex technology is not necessary since the networks involved are more straight-forward. There would however be a considerable administrative cost of managing the provision of data to Ofcom. This is estimated to require the equivalent of 0.1 FTE per CSP, which across 500 CSPs is estimated to represent a **£2.5m**[17] annual operational expenditure across the category.

As stated above, Category C CSPs already maintain a high baseline for monitoring and reporting, and as such there would be no direct cost impact arising from the provisions in this section of the Article.

Finally, there will be a greater cost to Ofcom for receiving outage information and reports, including potentially developing a sophisticated management system. This has not been quantified at this time.

[16] This is based upon approximately half of the category requiring investment of the order of £2.5m

[17] This is based upon £5k costs per CSP

Impact on Ofcom of onward reporting

The impact of the requirements on Ofcom to inform the public, other NRAs and, on an annual basis, submit an annual report on breaches to ENISA is largely independent of the scenarios defined above.

Disclosure to the public is not anticipated to represent a direct cost to any party as existing communication channels exist, such as DCMS and Ofcom websites. In addition, any notification to other European NRAs or to ENISA itself can be performed through existing channels.

The production of an annual report on breaches is not anticipated to present a cost to CSPs. Ofcom anticipates that the work would take two months of activity in compiling, reviewing and approving the report each year and require the resources equivalent to £7,000 in total per annum.

Category of CSP	Low	Medium	High
A	Negligible	Negligible	£10m capital
B	Negligible	Negligible	£2.5m per annum
C	Negligible	Negligible	Negligible
Ofcom[18]	£50k per annum	£50k per annum	>£50k per annum

Table 4-9: Summary cost of regulation of Article 13a(3) per Category of CSP

[18] From the combined cost of managing incident reports and responding to incidents as well as the annual reporting to ENISA. For the high scenario there would be a greater resource required to respond to incidents.

4.5 Harmonising measures

Article 13a(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).

4.5.1 Discussion

The provisions within Article 13a(4) allow for the further supplementation to the preceding provisions. Therefore there is no explicit impact arising from this article at this time.

There are a number of harmonising measures that are expected to be developed in the near future. These may include:

- Notification threshold – to define the threshold for ‘significant incidents’ to be notified to Ofcom under Article 13a(3), and the requirements for annual reports to ENISA.
- Standard for controls – to define an EU-wide standard of appropriate measures to guarantee the integrity of networks under Article 13a(2); this could be of a form and content similar to ND1643 or ISO27011.
- Standard for risk management – to define the specific risk management procedures required for compliance with Article 13a(1), for instance making reference to ISO27001.

The additional impact of any of the above measures has effectively been considered within Sections 4.2 to 4.4.

4.6 Implementation and enforcement

The provisions within Article 13b deal with the powers of Ofcom to investigate, audit and enforce compliance with the provisions of Article 13a. In terms of implementation scenarios the sub-articles of 13b are intimately interlinked, for this reason they will be considered and their impact assessed as a whole within this section.

> **Article 13b(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.
>
> **Article 13b(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.
>
> **Article 13b(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.

Within the Consultation (Ref [1]) it was noted that “such instructions [arising from 13b(1)] could be issued to address perceived failure in relation to risk management (and appropriate actions on resilience for network providers).”

It is possible to see this provision as broadly equivalent to the Information Commissioner’s Office powers to issue an Enforcement Notice, in that the organisation in question will be bound to compliance.

Similarly the powers defined by Article 13b(2)(a) are broadly equivalent to the Information Commissioner’s Office power to issue an Information Notice, with the additional support of Article 13b(2)(b) which allows for an independent audit of compliance to be made.

Finally, the power to investigate given by Article 13b(3) essentially provides the vehicle for the issuance of such requests for information, demands for audit and binding instructions. The Consultation (Ref [1]) noted that "the trigger for such an investigation would be if Ofcom had reasonable grounds to believe that a company was in breach of its obligations under the provisions under Article 13a(1) and Article 13a(2)."

4.6.1 Possible scenarios for implementation

The scale of possible implementations is simply dependant on the number of investigations implemented by Ofcom:

Degree of regulation	Description
Low	Ofcom would have a high threshold at which an investigation would be triggered, and as such would not assign any extra resource. In this case it is anticipated that only one investigation would occur per year.
Medium	Ofcom would be anticipating two to four investigations per year, and would require an extra resource to manage these investigations through the process.
High	Ofcom would be anticipating in excess of five investigations per year, and would require a significant extra resource to manage these investigations at each stage of the process.

Table 4-10: Implementation scenarios of Article 13b

The progression from request for information, demand for audit and issuance of binding instructions is essentially to be seen as a scale of escalation to the point that Ofcom is satisfied with the CSP's response. In that way, it is not supposed that all investigations will necessarily lead to either audits or instructions.

4.6.2 Current baseline

At present there is no NRA that issues binding instructions exclusively to PECN or PAECS providers or on the specific of matters of risk assessment, resilience or notifications of breach. Therefore the analysis of current baseline is not relevant.

It should be noted that CSPs are currently subject to independent audits for instance as part of Certification to ISO27001. However, these audits are generally broad-based whilst it is envisaged that the audits demanded as part of the new powers will be focussed and specific to an area of concern. Further the nature of any audit will depend and vary on the Article against which a non-compliance has been identified.

4.6.3 Additional impact of new provisions

Impact at Low scenarios

At the lowest end of the scale there would be no extra resource employed by Ofcom with no explicit extra cost. However, based upon analogous investigation activities of Ofcom, the management of a single investigation would require the resources equivalent to approximately **£36k**[19] over a five-month period.

The impact of an investigation on the individual CSP in question is difficult to quantify but it may be supposed that responding to an investigation may be the focus, though perhaps not the entire focus, of an individual's time, with the further support of specialists and senior managers as needed. Therefore, for a five-month investigation it is estimated that it may require resources equivalent to approximately **£25k**. These costs will of course only be incurred by the CSP being investigated/audited. Any further costs incurred by the CSP, in implementing improving measure to ensure compliance, are effectively covered within the findings of the earlier sections.

In addition, there is the direct cost to the CSP of a security audit. This will depend largely on the scale of concerns raised, but a focussed and specific independent audit may be of the order of **£30k**.

Finally the impact of binding instructions depends entirely on the nature of those instructions. However, since they will only be issued where there is a non-compliance with Article 13a the additional impact of such instructions is effectively covered by the analysis for those provisions.

Impact at Medium scenario

For the Medium and High scenarios the costs rise simply in proportion to the number of investigations and audits performed. These are demonstrated in Table 4-11 for four and ten investigations respectively.

Category of CSP	Low	Medium	High
A	£55k per annum	£220k per annum	£550k per annum
B			
C			
Ofcom	£36k per annum	£144k per annum	£360k per annum

Table 4-11: Summary cost of regulation of Article 13b per Category of CSP

[19] Ofcom have estimated, based upon the most analogous investigations Ofcom performs into other compliance issues, this would require an approximate 0.4 FTE at Principal level and 1.6 FTE at Associate level for 5 months for each investigation, which equates to a total cost over for each 5-month investigation of £36k.

4.7 Background resourcing

It has been noted by DCMS and Ofcom that to allow for a 'proactive' approach to be taken a background level of activity is required to keep in touch with the topic, the people and the policy developments, to attend ENISA, EC and UK Government and UK stakeholder meetings. To complete such activity it is anticipated that resourcing within Ofcom of approximately £55k per annum will be required.

Category of CSP	Low	Medium	High
A B C	None	None	None
Ofcom	£55k per annum	£55k per annum	£55k per annum

Table 4-12: Summary cost of background resourcing for Ofcom

5 Conclusions

5 Conclusions

Across the board, providers are fulfilling the basic requirements of security and integrity. In particular, appropriate measures are implemented covering the majority of the key control areas and their selection is based to some extent upon risk management decisions.

The acceptable risks to a provider are driven by the commercial requirements for service availability and network security. Frequently this means the use of service level agreements for suppliers or wholesale customers, or customer satisfaction indices for retail customers. Therefore a key area for potential improvement within the sector is compliance with specific technical standards where appropriate.

It is likely that the implementation of the new provisions will make use of, and enhance, existing legislation, regulation and information exchanges such as those reporting requirements arising from the Digital Economy Act 2010, and the forums in place under the remit of the Centre for the Protection of National Infrastructure.

The current operational expenditure for risk, security and incident management is assessed to be of the order of £200m per year across network and service providers. There exists considerable investment in technical measures and systems both within the networks and within operational support systems – however it has not been possible to quantify expenditure on ‘security’ elements as they are intrinsically linked to the network itself and are not viewed by providers as separate security expenditure.

The resulting additional impact of the regulations that will follow from Article 13a and b will depend critically on the stringency of those regulations. Table 5-1 anticipates the most likely scenarios and summarises the direct cost impact on Ofcom and the CSPs.

The Government’s preferred approach, as set out within the DCMS consultation (Ref [1]) is for light-touch regulation, and hence the additional impact as a result of the implementation of these regulations is expected to be modest. In addition, based upon the number of Significant and Major incidents that are believed to occur it is possible that a moderate number of investigations will need to be performed. As a result it is estimated that Ofcom will incur operational costs of £250k per annum, while CSPs will incur operational costs of £220k per annum.

If more enhanced regulations are implemented (e.g. under the medium scenario), in particular the mandating of particular standards across the market, then the impact is likely to be far greater. In particular small providers would be estimated to incur disproportionate costs of up to £18.5m in the first year, with considerable ongoing operational costs thereafter.

5 Conclusions

Article	Anticipated Degree of Regulation	Cost impact on Ofcom	Direct cost impact on CSPs	Benefits and other comments
13a(1)	Low or Medium	None	Application of Medium requirements to all (small) CSPs could cost £6m per annum	Improved and harmonised risk management across the sector
13a(2)	Low or Medium	None	Application of Medium requirements to all (small) CSPs could cost £12.5m in first year with additional operating costs in following years	Improved security of interconnecting networks, allowing for greater assurance between CSPs Reduction of significant outages, resulting in a more reliable service for the customer
13a(3)	Medium	£50,000 per annum	Negligible	Improve awareness of and response to significant incidents Concerns over commercial confidentiality and reputational image
13a(4)	N/A	None	None	-
13b	Medium	£145,000 per annum	£220,000 per annum	-
Background resource	N/A	£55,000 per annum	None	-
Total	N/A	£250,000 per annum	At Low - £220,000 per annum At Medium - £12.5m in first year, in excess of £6.22m thereafter	-

Table 5-1: Summary potential impact of Article 13

INTENTIONALLY BLANK

A Appendix

A Appendix

A.1 Definitions

The Communications Act 2003 defines an Electronic Communications Network:

> “(a) a transmission system for the conveyance, by the use of electrical, magnetic or electro-magnetic energy, of signals of any description; and
>
> “(b) such of the following as are used, by the person providing the system and in association with it, for the conveyance of the signals—
>
> > (i) apparatus comprised in the system;
> >
> > (ii) apparatus used for the switching or routing of the signals; and
> >
> > (iii) software and stored data.”

An Electronic Communications Service is defined as: “a service consisting in, or having as its principal feature, the conveyance by means of an electronic communications network of signals, except in so far as it is a content service.”

A Public Electronic Communications Network (PECN) is defined as: “an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public”

A Public Electronic Communications Service (PECS) is defined as: “any electronic communications service that is provided so as to be available for use by members of the public.”

A Publicly Available Electronic Communications Service (PAECS) is interpreted as having the same meaning as a PECS.

In this report we define a Communications Service Provider (CSP) as a provider of one of, or a combination of, PECNs, PAECSs or broadcast services.

In this report the term “security” refers to the concept of information security, which is concerned with the safeguarding of one or more of the following properties of ICT:

- confidentiality of information or data;
- integrity of information or data;
- availability of information, data or services.

A.2 References

[1] DCMS – Implementing the revised EU Electronic Communications Framework: Overall approach and consultation on specific issues, September 2010. (http://www.bis.gov.uk/assets/biscore/business-sectors/docs/i/10-1132-implementing-revised-electronic-communications-framework-consultation.pdf)

[2] DCMS - Implementing the revised EU Electronic Communications Framework: Impact assessment, September 2010. (http://www.bis.gov.uk/assets/biscore/business-sectors/docs/i/10-1133-implementing-revised-electronic-communications-framework-impact.pdf)

A Appendix

[3] BS25999-1:2006 Business Continuity Management. Code of Practice; BS25999-2:2007 Specification for Business Continuity Management

[4] CESG Security Procedures – Telecommunications Systems and Services – Issue No: 1.0 – July 2009

[5] Communications Act 2003 (www.legislation.gov.uk/ukpga/2003/21/contents)

[6] Data Protection Act 1998 (www.legislation.gov.uk/ukpga/1998/29/contents)

[7] Digital Economy Act 2010 (www.legislation.gov.uk/ukpga/2010/24/contents)

[8] Digital Economy Act 2010 Infrastructure Report (http://stakeholders.ofcom.org.uk/binaries/consultations/uk-comms-infrastructure/summary/uk-comms-infrastructure.pdf)

[9] Electronic Communications Framework Directive (2002/21/EC) (http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf)

[10] Electronic Communications ePrivacy Directive (2002/58/EC) (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML)

[11] Freedom of Information Act 2000 (www.legislation.gov.uk/ukpga/2000/36/contents)

[12] ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems – Requirements

[13] ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management

[14] ISO/IEC 27011:2008 Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

[15] Ofcom – Facts & Figures (http://media.ofcom.org.uk/facts/)

[16] Ofcom – Communications Market Report (http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/)

[17] NICC ND 1643 v1.1.1 (2009-09) Minimum Security Standards for Interconnecting Communications Providers (http://www.niccstandards.org.uk/files/current/ND1643%20%20Minimum%20Security%20Standards%20v1%201%201.pdf)

[18] PWC 2010 Information Security Breaches Survey – Technical Report (http://www.pwc.co.uk/eng/publications/isbs_survey_2010.html)

[19] Regulation of Investigatory Powers Act 2000 (www.legislation.gov.uk/ukpga/2000/23/contents)

[20] CMI – Disruption & Resilience – The 2010 Business Continuity Management Survey (http://www.managers.org.uk/research-analysis/research/current-research/BCM2010)

A.3 Glossary

Acronym	Definition
CNI	Critical National Infrastructure
CPNI	Centre for the Protection of National Infrastructure
CSP	Communications Service Provider
DCMS	Department for Culture, Media and Sport
(D)DoS	(Distributed) Denial of Service
DEA	Digital Economy Act 2010
ECF	Electronic Communications Framework
EC-RRG	Electronic Communications Resilience and Response Group
ENISA	European Network and Information Security Agency
EU	European Union
FTE	Full Time Equivalent/Employee
GSi	Government Secure Intranet
ICT	Information and Communications Technology
IEC	International Electro-technical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Provider
MVNO	Mobile Virtual Network Operator
NEAT	National Emergency Alert for Telecommunications
NRA	National Regulatory Authority
NSIE	Network Security Information Exchange
PAECS	Publicly Available Electronic Communications Service
PECN	Public Electronic Communications Network
PECS	Public Electronic Communications Service
SLA	Service Level Agreement
SME	Small and Medium Enterprise

A.4 Interview questions

Organisation Background

1. Name of Organisation:

2. Nature of Organisation: Does your organisation:

   directly own/manage or support any electronic network equipment:

   utilise fixed or mobile infrastructure:

   provide services to members of the public or business customers:

3. Confirm scope of discussions (eg limited to core or access networks):

4. Please provide an indication of the size of your organisation:

   number of employees:

   number of subscribers:

   total annual revenue:

5. Confirm level of awareness of ECF Directive? If organisation provided a consultation response, did you contribute?

Risk Management

6. Does your organisation perform risk assessments against threats to the confidentiality, integrity and availability of the services provided?

6a. If yes, does your organisation use any third parties for advice, guidance or comparison of threats or measures? Eg through CPNI Info Exchange or other.

7. Has your organisation completed an assessment of compliance (or gap analysis) against ISO27001 – Specification for Information Security Management Systems with a scope that includes communications networks and services provided?

7a. If no, then confirm the existence of the following:

   Information Security Policy

   Risk Assessment Methodology

   Governance and Accountability for risk management decisions

8. Is information security risk management integrated with Enterprise risk management, or driven by business requirements (eg by business ownership of accepted risks)?

9. Has there been a maturity assessment of the risk management framework? (eg using IAMM or similar – Initial, Established, Business Enabling, Quantitatively Managed, Optimised)

10. What specific security roles are identified without your organisation? Are these dedicated or shared roles? At what level do these roles report (in relation to the organisation's governing Board)?

Quality of Service/Availability considerations

11. Are there Quality of Service or Availability levels defined (targeted) for all or particular services? How is this assessed and maintained?

12. How do you calculate availability figures and how do you take account of major disruptive events in their calculation?

13. What approaches are employed to protect interconnect resilience against unwanted traffic like spam or DoS attempts?

14. Are mechanisms in place to identify and limit/disconnect sources of excessive bandwidth use by peering partners or customers?

15. To what extent, and where, are separacy, diversity and redundancy deployed within the network?

Standards and Compliance

16. Has your organisation completed an assessment of compliance (or gap analysis) against any of the following technical standards:

    ISO27002/ISO27011

    ND1643 (NICC Minimum Security Standards)/CESG Telecommunications Systems and Services

17. Would your organisation value an EU-wide standard covering security & resilience for communications networks?

18. Are compliance (procedural and technical – eg Pen Tests) assessments made on a regular basis to ensure security policies and procedures are being followed?

Supplier Management

19. Do third-party agreements/contracts routinely include security clauses? Are these enforced, monitored and audited?

20. If you procure network bandwidth or services from a third party, can you confirm whether there are any specific measures (eg SLAs) regarding service availability?

21. Do third-parties themselves perform security activities on behalf of your organisation?

Incident Management

22. When there is a breach of security, in particular a breach of availability of a service, is there a defined process for dealing with such a scenario? What information is recorded?

23. Are interfacing parties informed and involved when responding to a breach (of availability or integrity)?

24. Are investigations into incidents recorded in formal reports, assessing impact and documenting remedial actions?

Annual Spend on the above

25. Please confirm approximate annual spend on security resources and processes, in particular on the above activities. Please confirm this amount as a percentage of your total annual revenue?

26. Are there any major planned investments in the next two years that will effect this?

Please feel free to provide any further comments on the above or on Articles 13a and 13b of the ECF

About Detica

Detica delivers information intelligence solutions to government and commercial customers. We help them collect, exploit and manage data so they can deliver critical business services more effectively and economically. We also develop solutions to strengthen national security and integrity.

We integrate and deliver world-class solutions to our customers' most complex operational problems – often applying our own unique intellectual property. Our services include cyber security, managing risk and compliance, data analytics, systems integration and managed services, strategy and business change and the development of innovative software and hardware technologies.

Detica is part of BAE Systems, a global defence, security and aerospace company with over 100,000 employees worldwide. BAE Systems delivers a full range of products and services for air, land and naval forces, as well as advanced electronics, security, information technology solutions and customer support services.

For more information contact:

Detica Limited
Surrey Research Park
Guildford
Surrey, GU2 7YP
United Kingdom

+44 (0) 1483 816000

E: info@detica.com

www.detica.com