Department
for Business
Innovation & Skills

CALL FOR EVIDENCE ON PROPOSED EU DIRECTIVE ON NETWORK AND INFORMATION SECURITY

Summary of Responses

SEPTEMBER 2013

About this consultation

To: **All interested parties**

Duration: **From 22/05/13 to 21/06/13**

Enquiries: **Cyber Security Team**
Department for Business, innovation and Skills
1 Victoria Street
London SW1H OET

Tel: 020 7215 8566
Email: cybersecurity@bis.gsi.gov.uk

Contents

Introduction and Contact Details

This document is the summary of stakeholder engagement and official responses to the Call for Evidence on the proposal for an EU Directive on Network and Information Security.

It will cover:

- The background to the Call for Evidence
- A summary of the responses to the Call For Evidence and other stakeholder engagement on the Directive
- Details of next steps.

Further copies of this report and the consultation paper can be obtained by contacting the Cyber Security Team at the address below;

Cyber Security Team
Department for Business, Innovation and Skills
1 Victoria Street
London SW1H OET

Telephone: 020 7215 8566
Email: CyberSecurity@bis.gsi.gov.uk

This report is also available on the gov.uk website:

https://www.gov.uk/government/consultations/eu-directive-on-network-and-information-security-call-for-evidence

If you have further questions of the content of this paper or other issues related to cyber security, please contact cybersecurity@bis.gsi.gov.uk.

Background

The European Commission ran an online public consultation on ‘Improving NIS in the EU’ between 23 July and 15 October 2012. The response of the UK Government to this consultation can be found at the following weblink;

http://www.bis.gov.uk/assets/BISCore/business-sectors/docs/u/12-1222-uk-response-ec-consultation-network-information-security.pdf

The European Commission published a proposal for a Directive for Network and Information Security on 7th February. This was accompanied by a cyber security strategy (or ‘Communication’) which contains non legislative measures on a broad range of issues. These documents can be found on the European Commission website;

http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

In the Explanatory Memorandum accompanying the proposed Directive, the Commission states ‘The aim of the proposed Directive is to ensure a high common level of network and information security (NIS). This means improving the security of the Internet and the private networks and information systems underpinning the functioning of our societies and economies.’

The Department for Business, innovation and Skills (BIS) launched a Call for Evidence on the proposals on 22nd May 2013, which closed on 21 June 2013. The Call for Evidence sought information on the potential impact the measures in the proposed Directive would have on UK stakeholders. This document is a summary of the responses BIS received as part of this process. This evidence, in addition to that gathered in discussions, and the BIS workshop held on these issues with a range of interested parties, will help to assist the UK’s position in the ongoing negotiations at EU level and feed into a qualitative impact assessment.

Summary of key points in the proposed Directive

The proposed Directive covers the following main issues:

- It obliges all Member States to produce a national cyber security strategy and establish a CERT and a competent authority for cyber security.
- It mandates information sharing between Member States, as well the creation of a pan-EU cooperation plan and coordinated early warnings for cyber incidents.
- It mandates compulsory reporting of security breaches that have a significant impact on the provision of core services. Sectors that this would apply to include public administration, the finance, energy, transport and health sectors, as well as to ‘enablers of internet society services’ which includes app stores, cloud service providers, social networks and e-payment providers.

- Stakeholders would be required to report to the ‘national competent authority’ that would enforce the Directive. This competent authority would be given the powers to introduce sanctions, initiate audits and make public details of breach reports.
- It obliges Member States to encourage the use of standards and/or specifications relevant to network and information security.

Evidence Base

This paper will take into account views and comments provided to the UK government by UK stakeholders. In practice, this data comes from three sources;

A. The Call for Evidence

Responders to the call provided a range of views on the measures and potential impact and this information forms part of the evidence base for this paper.

Following the closure of the Call for Evidence, all submitted responses were analysed by BIS. In regards to this paper, text relevant to different aspects of the directive were flagged and categorised to the categories used in this paper.

As noted, the Call for Evidence was focused on providing evidence for use in the UK Government IA. The questions and proposed response template were not specifically tailored to the categories set out in this paper – responses were therefore varied in the categories that they discussed.

B. 22nd May 2013 Workshop

BIS held a workshop specifically on the directive, open to the sectors that would be affected by the proposed directive. The summary of the group discussions held at this event forms part of the evidence base for this paper.

C. Meetings

BIS has held meetings with stakeholders who expressed a direct interest in the Directive. The comments arising from these meetings forms part of the evidence base for this paper.

Categorisation

All submitted evidence was analysed to see if it contained text that had relevance to one of 14 categories. The categories broadly fall under two groupings.

– A-E focused on the wider picture of the directive, looking at the stakeholder view of the overall EU strategy, current requirements and the benefits and costs of the overall directive.

CATEGORY	DESCRIPTION
CATEGORY A	Developing an effective mechanism at EU level to address the different levels of capabilities and preparedness to ensure a common high level of protection in all the member states
CATEGORY B	Current mandatory and voluntary reporting mechanisms of NIS incidents
CATEGORY C	The practicalities of implementing the Directive
CATEGORY D	Potential benefits of the Directive
CATEGORY E	Potential costs of the Directive

– F-N focused on actual measures that the proposed directive would impose on UK stakeholders.

CATEGORY	DESCRIPTION
CATEGORY F	The scope of the Market operators as defined in Annex II of the proposed Directive
CATEGORY G	The inclusion of information society services in the scope of the Market Operators as defined in Annex II of the proposed Directive
CATEGORY H	The exclusion of micro enterprises from the scope of the Market Operators, as defined in Annex II of the proposed Directive [including comments on SMEs]
CATEGORY I	Member States to develop a National NIS strategy and a Computer Emergency Response Team (CERT), and establish a National Competent Authority to enforce the

CATEGORY	DESCRIPTION
	measures introduced in the Directive
CATEGORY J	Member States to form a cooperation network on NIS risks and incidents and create a secure information-sharing system
CATEGORY K	Market Operators to take appropriate technical and organisational measures to manage the risk posed to the security of their network and information systems and to notify to competent authorities incidents having a significant impact on the security of the cores services they provide
CATEGORY L	The threshold that incidents would need to be notified
CATEGORY M	That the NCA would have the power to issue binding instructions, audit and deliver sanctions to market operators and public administrations
CATEGORY N	That Member States encourage the use of standards and/or specifications relevant to network and information security

Range and scope of evidence

All direct quotation and references to UK stakeholder engagement is anonymous in this paper. References therefore do not indicate the name, sector and size of the organisation.

Any views expressed in this paper are representative of the views that UK stakeholders provided to BIS during this process. This is not a policy paper and the views contained within do not necessarily reflect the UK Government policy position on the proposal for an EU Directive on Network and Information Security.

Summary of UK Engagement

To complement the written Call for Evidence, BIS officials also met representatives from a range of industries and sectors, both in bilateral discussions, wider roundtable events, and a specific workshop on the proposed Directive. These have been important in gathering views on the proposals, and we have been particularly grateful for those events organised externally to which we have been invited. These sessions have been thought-provoking and have helped to inform the Government's position on the proposals.

A. The Call for Evidence

The consultation ran between 22nd May and 21st June. In total BIS received 88 responses to the Call for Evidence. The Call for Evidence document can be found at the following weblink;

https://www.gov.uk/government/consultations/eu-directive-on-network-and-information-security-call-for-evidence

The written responses to the Call for Evidence were logged and filed upon receipt by the Department for Business, Innovation and Skills. The Cyber Security policy team then considered each response and noted where comments were made relevant to the 14 categories that this paper covers. As the Call for Evidence was not focused directly on these categories, responses ranged from covering most of the categories to others not providing text on any. This does not reflect the quality of the response.

SECTOR	RESPONSES
Provider of Information Society Services	22
Banking / Financial Services / Provider of Financial Infrastructure	19
Transport Sector	8
Energy Sector	8
Health Sector	6
Telecommunications Sector	6
Public Administration	5

SECTOR	RESPONSES
Regulatory Body	4
Policy Groups	3
Aerospace and Defence	2
Non sector specific Trade Associations	2
Information Security Consultancy	2
Media	1
Water Sector	1
Education	2
Insurance	1
Business Services	1
Industrial Process Control	1
No sector given / anonymous	3
Total[1]	**97**

In regards to this summary paper, we reviewed and analysed each response and noted where comments were made next to the 14 categories this paper covers

The following is a breakdown of the number of responses that provided evidence (either qualitative or quantitative) for each category;

[1] Some responses choose multiple options to define the sector that they operated in – the total for this section is therefore greater than the total number of responses.

CATEGORY	DESCRIPTION	No
A	Developing an effective mechanism at EU level to address the different levels of capabilities and preparedness to ensure a common high level of protection in all the member states	18
B	Current mandatory and voluntary reporting mechanisms of NIS incidents	28
C	The practicalities of implementing the Directive	10
D	Potential Benefits of the Directive	10
E	Potential Costs of the Directive	29
F	The Scope of the Market Operators as defined in Annex II of the proposed Directive	7
G	The inclusion of ‘providers of information society services’ in the scope of the Market Operators, as defined in Annex II of the proposed Directive	4
H	The exclusion of micro enterprises from the scope of the Market Operators, as defined in Annex II of the proposed Directive	5
I	Member States to develop a National NIS strategy and Computer Emergency Response Team (CERT), and establish a National Competent Authority to enforce the measures introduced in the Directive	7
J	Member States to form a cooperation network to share information on NIS risks and incidents and create a secure information-sharing system	12
K	Market Operators to take appropriate technical and organisational measures to manage the risk posed to the security of the network and information systems and to notify to the competent authority incidents having a significant impact on the security of the core services they provide	20
L	The threshold that incidents would need to be notified	13
M	That the NCA would have the power to issue binding instructions, audit and deliver sanctions to Market Operators	12
N	That Member States encourage the use of standards and/or specifications relevant to networks and information security	6

Where possible this summary document has tried to reflect the majority view but where a particularly important point was put across by a small proportion of respondents (for example, members of a particular sector) we have included these as well.

B. 22nd May 2013 Workshop

BIS held a workshop specifically on the directive, open to the sectors that would be affected by the proposed directive. (as listed in Annex II). The event was entitled ‘EU Cyber Security – An opportunity for Businesses to have their say’.

Following an initial ‘expressions of interest’ round (where over 200 organisations expressed an interest in the event), representatives from 73 organisations were invited to the workshop. These organisations were chosen to ensure the full range of sectors that would be affected by the Directive was represented and that there was a mix of organisations of different sizes present.

The event was held under Chatham House rules. It consisted of a series of presentations from BIS and organisations that had looked at the NIS Directive in-depth, and was then followed by a group discussion where participants were encouraged to put forward their views and position on the proposed measures.

The summary of the group discussions held at this event (ANNEX A) forms part of the evidence base for this paper.

C. Meetings

As part of the consultation process with industry, BIS looked to hold a number of one to one meetings to discuss the proposed directive and understand in more detail how the measures could affect an organisation.

In total, BIS held 29 meetings (both bilateral and with groups and associations) with organisations with an interest in the Directive. These meetings fell under the following categories;

SECTOR	RESPONSES
Internet Society Services	8
Public Administrations / Government	5
Banking/ Financial Sector	4
Telecommunications	3
Transport	3
Energy	2
Regulators	2
Legal	1
Other	1
Total	**29**

Views expressed at these meetings forms part of the evidence base for this paper.

European Commission Documents

The Commission have also published work in regards to stakeholder views of both Network and Information Security and of the Directive. As these documents are in the public domain and available to responders to the UK Government call for evidence, these documents have been noted in this section.

EU Consultation and Responses

One of the data sources for the Commission's Impact Assessment was a consultation held by the Commission in October 2012. The UK Government participated in this consultation and its response can be found at the following weblink;

http://www.bis.gov.uk/assets/BISCore/business-sectors/docs/u/12-1222-uk-response-ec-consultation-network-information-security.pdf

In terms of their public consultation the Commission received 169 responses in total of which 97 were classed as individuals and the others were answering on behalf of an organisation or an institution. Of 96 respondents that identified themselves either as a private company or as a business association in one of the fields provided, only 16 and 15 respectively were in the sectors that will be affected by the NIS Directive. Hence there appears to be a slight imbalance in the sample which could have also influenced the selection of the sectors suggested for inclusion under the NIS Directive as this appears to be heavily based on this public consultation.

EU Impact Assessment

The Commission published an Impact Assessment to accompany the draft Directive. This Impact Assessment provides a good outline of the problems to be addressed and the potential reasons for the current underinvestment in security and resilience spending by companies. However, this document is not as comprehensive as we might have hoped, and some questions remain. Notably there are discrepancies between the lists of market operators in the Impact Assessment and the Directive and that we would want to see further clarity on key assumptions made during the analysis, such as the assumption of an initial natural increase of 8.4% in the ICT security spending and the assumption that between 40% and 70% of additional required ICT security spending will not be caused by the NIS Regulation.

The UK government provided a list of queries to the Commission in regards to the EU Impact Assessment. This list can be found at **Annex B.**

Responses to specific questions

CATEGORY A

Developing an effective mechanism at EU level to address the different levels of capabilities and preparedness to ensure a common high level of protection in all the member states.

Summary

- Stakeholders, even when highly critical of the proposed Directive, saw that there was a significant role for the EU to play in addressing Network and Information Security across the Member States.
- Stakeholders, particularly multinational organisations, were keen to ensure that a fragmented regulatory regime did not emerge in Europe and/or globally that would add costs to ensuring compliance.
- Some stakeholders referenced that this was a global issue and that the EU had a role to play in developing the global solution to Network and Information Security
- Stakeholders recognised the importance of national competence and that it was important for any EU activity to recognise this competency and not detract from best practice identified at a national level.

Stakeholder Comments

‘The Sector would welcome efforts to harmonise cyber security policy for the sector across different nation states and this needs to take into account activities in countries beyond the EU.‘

‘…believes to ensure the prosperity of EU Member States that the use of the internet for ever increasing business transactions is a safe and secure environment. Therefore effective measures to defend, monitor, respond and report, firstly on a national basis and then through sharing on an international basis is essential.’

‘…supports the objective of improving resilience and reducing online crime. This will improve consumer confidence and widen inclusion in the digital economy, essential to support activities such as smart metering and e-commerce’

‘There is little information in the proposal to indicate alignment with other bodies outside of the EU who are also developing approaches to cyber security such as in the US, and that are likely to impact our members.’

‘[While] the draft NIS directive may improve capabilities for governance, readiness and response, particularly in governments, it may not reduce the number of incidents or their severity.

‘There is no wish to see a highly fragmented regulatory regime across Member States as has been seen with other Directives… The EU role should be appropriately balanced and the importance of activities at a national level recognised.’

‘We welcome the efforts of the EU to harmonise the fragmented network information security legislation that is currently in place across the EU, which will be helpful to most EU businesses with the Single Market’

‘…supports the principles and implementation of the Directive that will lead to a strengthening and consistency of cyber defence controls across all EU member states.’

‘We welcome any activity which draws attention to cyber threats and enables progress across Member States and operators of critical infrastructure.’

‘We are supportive of the intention of the Directive to achieve a step change in the implementation of cyber security across the EU, and the desire to achieve a consistency of approach across business sectors and member states.’

‘recognise the wider importance to the economy and society of having NIS risk management and mitigation measures in place’

‘…enhancing the situational awareness of critical infrastructure owners and operators would actually increase the security of personal information that is maintained on company networks and systems. Improved information sharing would benefit individuals' privacy protections, not detract from them.’

CATEGORY B

Current mandatory and voluntary reporting mechanisms of NIS incidents

Summary

- Stakeholders focused on the value of voluntary, trust based approaches noting specifically the Cyber Security Information Sharing Partnership (CISP), and the Centre for Protection of National Infrastructure (CPNI) Information Exchanges.
- Some sectors were already obliged to report incidents that would involve a cyber security event under current reporting structures and mechanisms. For example, an incident in the energy sector would be reported to the energy regulator, Ofgem, but would not be isolated to just cyber security events.
- Some sectors did not have mandatory reporting requirement for incidents. Organisations in these sectors could create informal relationships with the regulators or build in reporting into their business plan/governance.

Stakeholder Comments

‘Within the UK there are already a number of effective information sharing forums, both formal and informal, which should be encouraged and not subject to greater regulatory pressure.’

‘In most markets we operate as a regulated industry and report as required by our industry obligations. We have no independent reporting requirement that is specific to security incidents’

‘As a supplier to UK government we are contractually obliged to report security breaches’

‘We consider voluntary, trust based, reporting by industry sector to be more sensible. This happens already in key sectors such as the financial sector, defence and aerospace.’

‘We operate closely with CPNI and in accordance with the processes governing Critical National Infrastructure (CNI) as develop by the Government. We have found this to be an effective means of facilitating information sharing and lesson learning within a 'secure environment'

‘[We are] a participant in the newly formed CISP and has in the past reported incidents to CPNI for both analysis and response purposes. [We] also participate in one of the CPNI Information Exchanges.’

‘We provide informal and ad hoc reporting to our regulator, sponsoring department and CPNI where a security incident affects our ability to deliver committed services to our customers.’

‘The draft directive should embrace principles that both resonate with the owners and operators of critical infrastructure and are flexible enough to address a rapidly changing threat environment’

‘…we share information with other [organisations in our sector] in Europe to gain better situational awareness of ad-hoc cyber threats, in an effort to prevent these becoming real incidents. Other [companies] also do this, respecting their own potential national security issues’

‘We would share appropriate and relevant information with the communities with whom we work (e.g. other registries, the UK CERT Forum, the Network Security Information Exchange and Project Auburn/CISP)’

‘…contacting UK authorities is already in our Business Continuity Plan for significant business continuity incidents.’

‘We provide information in good faith where we believe it will be of use/interest to other CPNI/CISP members in the transport sector and where we think CPNI itself may have an interest or be able to provide us with help.’

CATEGORY C

The practicalities of implementing the Directive

Summary

- All stakeholders agreed that it was impossible to fully predict the full impact and issues of implementing the Directive without further information (notably on the thresholds for reporting and the scope of organisations affected by the proposed measures)
- Organisations were concerned that, without full harmonisation, a fragmented compliance regime could form and that they would need to deal with different requirements in different Member States.
- Stakeholders raised concerns on the expertise and capability both at a National level and at an EU level. For example, a comment was made that it took 3 years for the US CERT to reach full capability. There was a perceived risk of implementing the Directive when key bodies were still developing their expertise in this area.
- It was important that there was harmonisation between the Directive and other EU regulations and Directives, notably the EU Data Protection Regulation.
- It was essential that a safe, secure reporting structure was in place; many stakeholders raised significant concerns on the safety of data once submitted.

Stakeholder Comments

'…detailed consultation is needed with experts from relevant industries to consider the practical implications arising from the current text of the proposed Directive

It is considered that any such Directive should have minimal financial and resource implications.'

'We remain concerned that, if the directive is not implemented wisely, another 'quango type' agency will give rise to more confusion'

'…should strike a better balance between providing protections to businesses, large and small, yet not burdening the smallest businesses with disproportionate processes and costs'

'There must be harmonisation of requirements and obligations between this Directive and other relevant EU Regulations and Directives. In particular there is potential conflict with the EU Data Protection Regulation that is currently under discussion. Consistency with initiatives under development in other parts of the world is also to be encouraged.'

'Many critical areas are left open for the Commission to issue rules and guidelines which means that it is ultimately impossible to fully assess the impact of the proposals.'

‘…it’s vital that the companies do not adopt a ‘tick box’ approach to security and understand that truly effective cyber security is a combination of having the right people, processes and technologies in place.’

‘Today, there is no clear way to classify incidents and report them in a manner which helps the recipient of such data understand the implications in a fast simple approach.’

‘…building new institutions (i.e. National Competent Authorities and CERTs) takes time. Incident reporting requirements should focus on public administrations first and then be scaled to include private sector critical infrastructure once such a model has been successfully established.’

‘It is difficult to determine the precise time to create an incident report, as this could vary considerably depending on the data required to be submitted’

‘The more potentially complex and significant the more costly and (potentially) slower the incident reporting will be.’

CATEGORY D

Potential Benefits of the Directive

Summary

- Stakeholders struggled to connect the outcomes of the Directive with the objectives defined in the EU Cyber Security Strategy.
- Stakeholders supported the development of national NIS capabilities, namely the creation of National CERTs and national Cyber Security Strategies. They saw advantages in creating a more structured framework between Member States and the EU, provided it did not infringe on best practice being performed in the UK at a National level.
- With regard to reporting and information sharing, this had to occur in a two-way fashion; the National Competent Authority and the EU would need to share relevant and structured feedback to enable organisations to action a meaningful change.
- The development of a Pan-European threat picture was seen as a positive element – however there were concerns that the framework put in place would be too slow and unwieldy to act sufficiently quickly to reduce the impact of any incident.

Stakeholder Comments

‘If implemented effectively and efficiently, consumer confidence could grow.

Improved situational awareness that could come from information sharing will help to assign resources to protecting critical assets.’

‘Firms will see no benefits from reporting if the information flow is seen as going in only one direction (i.e. from the private sector to the authority), and if there is no confidence in the ability of the authority to act effectively on that information’

‘It is possible that a pan-European threat picture could result in better response. Frankly we are sceptical that such a thing can respond sufficiently quickly to result in any reduction in the seriousness of incidents’

‘If information sharing was effective we might be able to reduce some costs we spend on threat intelligence, however it would take some time (a few years) before we would be comfortable with doing this.’

‘As the Directive may result in further scrutiny of incidents it could potentially reduce the seriousness of incidents experienced by organisations. This is, however, difficult to quantify.’

‘We perceive some value in developing limited but very highly centralised capability that may be relied upon when HMG and the business deem it appropriate to communicate directly with [appropriate EU institutions].’

‘Yes it may if by reporting pro-active action is taken to reduce or prevent attacks launched from within the EU or other co-operating nation states.’

‘No. It is possible that by the wider reporting of security incidents and vulnerabilities that there is a net increase in the number of incidents unless some pro-active value can be obtained from shared intelligence such as attack signatures or preventative measures for emerging threats.’

‘…well crafted and appropriate EU requirements could drive companies to devise specific NIS solutions in Europe, which could then be scaled up and deployed efficiently and helpfully across their global networks.’

CATEGORY E

Potential Costs of the Directive

Summary

- Stakeholders indicated that they needed further details not available in the proposed Directive to fully understand potential costs to their organisation (such as the threshold for reporting, and information on the powers /capabilities of the National Competent Authority)
- The primary concern was that mandatory reporting and the potential for audit and sanctions would penalise organisations with strong NIS capabilities who would detect more advanced intrusions on their network and benefit organisations who have a minimum level of capability (and not able to detect advanced intrusions). This could have the effect of lowering NIS capability as organisations trend towards a minimum tick box compliance exercise and not develop strong cyber security hygiene.
- Stakeholders flagged that mandatory reporting would create a compliance culture; this would stifle voluntary information sharing and resources that would be allocated to developing cyber security capability would be reallocated to employing legal teams to analyse each incident.
- Significant concerns were raised by stakeholders on the NCA capability to both audit and impose sanctions. These, in turn, could increase costs and divert more resource to legal teams.

Stakeholder Comments

‘What is needed is a proactive preventative intelligence by industry sector, not a negative / punitive lag reporting to the EU. It is totally misconceived.

‘We are keen to avoid the risk of excessive regulation (through a duplication of existing requirements’

‘Prescriptive requirements could stifle innovative approaches, may lead to a 'tick box' approach to compliance and undermine effective collaboration between firms and industries’

‘At this stage it is not possible to state where the burden of this reporting will lie as it will depend upon the final scope and nature of the final implementation but is most likely to impact the IT department’

‘There are potentially significant reputational risks in incident reporting and disclosure. Our experience to date is that it works when trust is developed in well-known and relatively small groups.’

‘Additional EU mandatory controls will set an unwelcome precedent that other nations may follow and thereby harm our ability to maintain a secure operating environment’

‘The implementation of the Directive would also likely encourage and embolden additional reporting requirements in other parts of the world. Without harmonisation of such efforts, there will be an increase in cost, an exposure of operational information and details to a growing group of international regulators, which creates its own information security risks.’

‘The proposed directive risks a significant increase in the regulatory burden to network operators and providers of over-the-top services… may also increase barriers to entry and obstacles to the transition from micro-business to small-business’

‘Overall this proposal for a directive will, if implemented, probably increase [our] costs, and inadvertently encompass incidents that do not have a cyber security root cause.’

‘Providers with poor security policies may fail to detect many security incidents, and will therefore find the reporting requirements less burdensome than providers with better security practices.’

‘We are concerned that such a directive would place an unnecessary administrative burden on health and social care organisations public and private’

‘These policies could create a negative incentive for compliance and will result in fewer reports from those firms that currently have good practices, as they will be concerned with the increased risk profile and possible reputational damage.’

‘…the existing non-regulatory approach in the UK can help to promote open and transparent engagement between businesses and government… this has facilitated a secure and effective environment for sharing information. We think that the systems and processes laid out in the draft Directive could create additional costs with no material security or resilience benefit.’

‘EU based companies would become less competitive as we would have a higher cost base in order to comply with EU-specific security requirements.’

‘While we have some strong processes in place, as with any regulatory requirement, the level of effort/burden to support the due diligence required (depending on the nature of the obligation) would most likely see increased FTE costs, system costs and additional effort to meet the requirements of the obligation.’

‘The Directive could have significant negative consequences for our rights and freedoms, and for the fight against cybercrime.’

CATEGORY F

The scope of the Market Operators as defined in Annex II of the proposed Directive

Summary

- Stakeholders requested further clarification on the scope identified in Annex II and the rationale behind why those sectors had been identified. They noted that this question was linked with the issue of the threshold for mandatory reporting and would need further information on both before reaching a definitive position.
- The scope was highly expansive and might inadvertently include companies and organisations that have no impact on critical infrastructure. Some stakeholders wanted the scope to be narrowed and be less expansive.
- The issue of supply chain was brought up and how this would interact with the sectors identified.

Stakeholder Comments

‘We cannot support the exclusion of software developers and hardware manufacturers from the requirements of the Directive as consistent approaches across these market operators are vital.’

‘Given the wide scope of 'market operator' as defined in the proposed Directive, this burden may be imposed on networks and services the availability of which has very little bearing on the Internet economy as a whole.’

‘Perhaps the Directive is too narrow given the limited number of market operators identified. Our operations have significant interdependence with our supply chains

A wider scope to more encompass the supply chain would better address the risk. The delivery of our core services is dependent on a spectrum of third party providers… which would not be subject to the requirements of the Directive.’

‘We do not know how the new term "critical service for society" has been established and how it will be defined and applied’

‘the proposed definition of 'market operators' may inadvertently include experimental platforms used in the establishment of national and international digital research infrastructures… would severely limit their capability to innovate and discover both new science and new ways to provide future services in both the academic and commercial sectors.’

‘A greater attempt should be made to restrict reporting and risk management requirements to those services whose disruption is likely to result in significant further disruption in the wider Internet economy’

‘The 'market operator' definition is overly broad, which could lead to uncertainty for businesses and weaken government's ability to manage risk.’

‘A characteristic of 'cyber is interconnectivity - we suggest that the Commission consider what the meaningful scope really is both in terms of market sectors and depth through the supply chain and clarify the Directive accordingly’

‘considers that the definition of 'market operators' is extremely broad and further clarification is required…further clarification of the types of service which fall within the scope of the new NIS requirements would be beneficial to avoid confusion when it comes to implementation’

CATEGORY G

The inclusion of information society services in the scope of the Market Operators as defined in Annex II of the proposed Directive

Summary

- Stakeholders saw introducing mandatory reporting to this sector as challenging – stakeholders failed to see where the benefits lay in mandatory reporting and argued that voluntary relationships would create more positive benefits.
- It was noted that the definition is highly expansive and could encompass a large number of information society services [most however noted that this was tied to the threshold set for reporting]

Stakeholder Comments

'…areas such as internet and cloud services, as several services, products are delivered and operated across an entire value chain by different suppliers and/or integrated with each other.'

'…in practice a significant proportion of information society services will satisfy this criteria, since it is in the nature of information products that they can in principle be processed and repackaged as components of further information services…'

'Attempting to include 'internet enablers' into such a reporting scheme will create a lot of data but this may not translate into actionable information to protect public safety.'

'…in the case of information society services, we believe that this goal may be better served through voluntary relationships founded on trust rather than legal compulsion'

'…the Directive should focus on critical infrastructure providers. Including so-called "internet Enablers,' e.g. in the proposed incident reporting requirement raises more challenges than benefits'

CATEGORY H

The exclusion of micro enterprises from the scope of the Market Operators, as defined in Annex II of the proposed Directive [including comments on SMEs]

Summary

- Stakeholders were generally positive that micro enterprises were excluded from the proposed directive.
- Concern was raised that the directive could still place significant burdens on SMEs, specifically when micro enterprises transition from a micro business to a small enterprise. It was important that the directive placed realistic and proportionate burdens on SMEs.

Stakeholder Comments

‘…we want to make sure that those smaller businesses such as cloud computing service providers, private health clinics, logistics services are protected, and that the compliance approach is proportionate.’

‘Although risk management and notification requirements do not apply to micro-businesses, thereby avoiding the worst barriers to entry that could have resulted from the Directive, the Directive may create obstacles to businesses transitioning from micro- to small-business status.’

‘…is particularly keen to ensure… that the important micro exemption is retained and that the approach is very much a risk-based one and reducing a potential disproportionate burden on small businesses.’

‘…most SMEs are cost sensitive and to require additional requirements will increase cost but may not increase protection. The only people to gain from a directive would be consultants.’

‘…mindful of smaller businesses outside the micro exemption that may be disproportionately impacted by these proposals.’

‘As soon as any internet-based service has got off the ground and employed its tenth person it will become subject to the Directive's reporting and auditing regime. The burden to small businesses is therefore potentially quite significant which may harm the agenda for innovation in the digital economy that both the UK Government and European Commission would like to see.’

CATEGORY I

Member States to develop a National NIS strategy and a Computer Emergency Response Team (CERT), and establish a National Competent Authority to enforce the measures introduced in the Directive

Summary

- Comments on this topic identified these measures as directly adding value to the objectives of the EU Cyber Security Strategy, and would help develop capability across the EU Member States.
- Concern was raised on potential duplication of reporting requirements between the National Competent Authority and existing sector regulators.

Stakeholder Comments

‘A competent body has the potential to streamline reporting or complicate it…

the US CERT was established in 2003 but it took about three years to grow its operational capabilities from initial operating capability to fully functioning national CERT.’

‘…the proposal to establish competent authorities and CERTs in every country is a practical step that will develop capability across the Union, as is the development of tools and mechanisms to promote cooperation between them.’

‘The creation of an additional regulator for companies [in the sector] would be of limited benefit to our customers, whilst introducing confusion and complexity into our investigation and reporting processes.’

‘…for each country to have a Cyber Security Strategy, a CERT and a platform from which to share information on cyber attacks… align well with the principles well defined in the UK Cyber Security Strategy and would have the desirable result of bringing the least capable EU countries up to a minimum standard.’

‘It seems sensible in an age of government cuts and austerity to use an existing and well established regulatory body to implement the provisions outlined in the proposed directive.’

‘…any requirements imposed by a new competent authority for network and information security are fully aligned with the strategic direction and requirements of existing UK regulators.’

CATEGORY J

Member States to form a cooperation network on NIS risks and incidents and create a secure information-sharing system

Summary

- Stakeholders, particularly multi national organisations saw the potential organisational benefits of this system, potentially removing the requirement to report in multiple countries when an incident occurred.
- Concern was raised on the safety of information that was shared on the cooperation network; organisations estimated that it would likely be sensitive and increased distribution in turn increased the risk that the information could be targeted.
- Organisations supported the informal networks and public/private networks that existed between themselves and government and welcomed the 'cooperation network' as establishing better communications between Member States and the Commission
- Stakeholders flagged that any cooperation network should establish two way sharing.

Stakeholder Comments

'[secure information sharing], information about sensitive matters relating to company or national security may be divulged to a wider audience than would be under the present 'need to know' arrangements.'

'We also have concerns about the Commission's, ENISA's and government's expertise and resources to fulfil tasks they would need to undertake under these proposals.'

'We'd like to see the creation of a public information service where the cyber centre becomes as well used as the 'Met Office' is for weather reporting. For example, consider a risk and treatment bulletin at the end of national news broadcasts.'

'We remain concerned about sharing information beyond our forum, through fear of exposing additional vulnerability or experiencing reputation damage. We would like to see more details on the supporting legal framework and information sharing requirements and processes at National and EU levels'

'While a company may appear to only incur small costs for reporting to one country, such as the designated NCA in the UK, there may be reporting requirements for an additional 27 member states that could vary in content, format and procedures.

Many governments have existing regulators for specific critical infrastructures and agencies that over see security requirements for government networks. Finding a way to bring these existing authorities into alignment and ensure that cyber security requirements are coordinated across these entities and the newly designated NCAs will be challenging.'

‘…before information is shared on an EU-wide basis, policy makers should do more to reassure organisations that sensitive information will be dealt with securely. This is due to the perceived lack of system security at both national and EU levels… policy makers should recognise that some businesses may be reluctant to admit to cyber attacks due to the risk of leaks and consequent reputational damage.’

‘…if Member States will be required to create NIS competent authorities in addition to the existing sector specific regulators… this would create duplicative compliance requirements adding to the companies' compliance costs.’

‘We support the private/public partnership advocated in the EU cyber security strategy document…. Will foster more information sharing and improve the bi-directional information flow and co-ordination from intelligence communities and government agencies that are tasked with gathering global intelligence.’

‘There should be an emphasis on trust and a two-way sharing of data, to help protect organisations from attacks, with reports made through anonymity’

‘Intelligence sharing should be used to perform trend analysis and horizon scanning, to encourage cross border cooperation with law enforcement agencies and to share live data for attacks that are taking place.‘

‘Reporting of security incident data through a chain to a central repository makes available substantial valuable data to carry out further attacks and represents a significant target.’

CATEGORY K

Market Operators to take appropriate technical and organisational measures to manage the risk posed to the security of the network and information systems and to notify to the competent authority incidents having a significant impact on the security of the core services they provide

Summary

- Stakeholders struggled to identify the exact impact that a mandatory reporting requirement would have – more information was required in regards to the reporting threshold.
- The primary concern raised was that introducing a mandatory reporting regime with potential sanctions following reporting would lead to less information sharing. Sanctions and audits would lead to a disincentive to report.
- Another issue raised was that mandatory reporting could cover incidents that are already reported to the sector regulator; this could lead to a duplication in reporting.
- There were concerns that mandatory reporting could also bring about increased legal costs as companies look to minimise their reporting through legal advice on a case by case basis.

Stakeholder Comments

'…legal teams would likely be brought into the process of reporting, with further associated resource implications'

'Mandatory reporting will probably lead to a reduction in reported incidents as the consequences of the reporting may be greater than the damage done by the attack so excessive effort will be placed on managing the reporting rather than learning from the events.'

'The mandatory reporting by all businesses… in a large number of industry sectors in a tight timescale with penalties for failure to do so, plus sharing of such data with and across the EU is unacceptable.'

'Perhaps the Directive is too broad with the requirements regarding market operators. There would arguably be benefit in addressing requirements of member states and agreeing standards prior to imposing requirements on market operators.'

'…incentivising voluntary cooperation and information sharing would be a more effective approach towards achieving the goals of increased capability levels across the EU'

'A typical incident could include many different people in different parts of the company for up to hundreds of human-hours.'

‘The classification of incidents should be proportionate to the risk and impact.’

‘Mandating incident reporting may also have the unintended consequence of stifling innovation and the development of good cyber security practice, particularly if costs are diverted towards simply complying with the reporting obligations.’

‘A cyber security program must not divert companies' resources towards satisfying compliance mandates, instead of improving security.’

‘We request clarity around incident reporting requirements, particularly around the management of data and how the protection of confidential information will be used, transmitted, stored, validated and audited. We believe the focus should be on proactively improving capability across the EU, rather than on mandatory reporting.’

‘We would propose a tiered approach of reporting for companies of different sizes and target-profiles combined with information sharing, meaning that significant incidents should be reported (defined by tier, for example similar to security standards for the payment and cards industry) and other incidents should be shared rather than reported.’

‘We would propose a more tiered approach of reporting combined with an information sharing. This is that our level of serious gets reported (defined by tier for example similar to PCI DSS) and that all else is shared rather than reported.’

‘…we anticipate a reduction in business effectiveness as management attention is diverted to verifying reported data… communications processes are diverted to new reporting requirements leaving less opportunity for useful reporting and the conversations that we have with customers, stakeholders and partners are focused on what happened in the past, rather than what we aim to deliver in the future. This is likely to have a negative impact on the positive culture we have established in our business. ‘

CATEGORY L

The threshold that incidents would need to be notified

Summary

- Stakeholders identified this as the key measure in the Directive; it directly affected the impact that the directive would have on organisations. As such, without further clarification of ‘significant impact’, stakeholders could not fully identify the impact the directive would have on their organisation.
- There was a variety of views on what the definition of significant impact would be. The general position was that it should be set sector by sector.

Stakeholder Comments

‘…clarification on which incidents should be widely reported to the EU, if every incident is reported vast resources will be required to analyse and prioritise remedial actions. It is considered that only major incidents… should be reported.’

‘[A high severity] incidents will usually cause a degradation of vital services for a large number of users, involve a serious breach of network security, affect mission critical equipment or services, or damage customer confidence’

‘Without impact criteria it is difficult to identify what is meant by a 'significant' incident, and to what type of asset this may apply.’

‘Even with the guidance provided terms such as 'core service' and 'significant impact' need to be better defined. These cannot be the same across all industry sectors.’

‘…the current draft Directive does not provide sufficient detail on how the threshold for reportable incidents is defined, including the basic question of what constitutes a "significant" incident or impact’

‘The threshold of what a significant impact constitutes should not be left to the implementing acts but needs to be defined in the directive . A useful definition of the term 'significant impact' would be "an incident that is not a routine or accidental breach of information technology compliance management policies but is anomalous and has the ability to create significant harm resulting in the loss of lives of the destruction of property."’

‘It's quite possible the Directive would be counter productive and encourage an organisation not to look for incidents. Incidents that are not detected don't get reported.’

‘This threshold is too broad and not well defined. In order to focus on the most prevalent risk, it is important to clarify and define the significance of the impact of an incident in the directive itself.’

‘We know from experience… that reporting (and having an agreed threshold/trigger) is extremely difficult.’

‘…want to make sure that thresholds to trigger reporting of incidents are appropriate to the sector.’

‘If an incident causes the market operator to operate its business in a way that is detrimental to the integrity of the data and services, it should be classed as a significant incident.’

Without further clarity and until we have carried out a full impact assessment of the specific requirements under the Directive, there could be unforeseen consequences that might impact on our organisation.

CATEGORY M

That the National Competent Authority would have the power to issue binding instructions, audit and deliver sanctions to Market Operators and Public Administrations

Summary

- Stakeholders focused on the measure that would allow the National Competent Authority to make public incidents without the permission of the initial organisation who filed the report. They commented that this could have major repercussions with reputational damage and create disincentives to proactively look for breaches above the minimum required standard.
- Stakeholders raised concerns on potential sanctions. They saw the potential sanctions and audits as disincentives to report incidents on a voluntary basis.

Stakeholder Comments

‘ if the National Competent Authority made obligation for reporting audits [this] could actually negatively impact security by exposing sensitive operational information to a broad range of individuals and organizations.’

‘Depending on the reporting within the sector, there could be a loss of public confidence in the whole banking sector which could affect all of the organisations with potential disastrous consequences to the public infrastructure.’

‘…sanctions should be proportionate to, and reflect, business turnover. They should also incorporate a warning system so that the business has one or two warnings first to give them an opportunity to improve their systems and helped towards compliance before any fines kick in.’

‘There is a significant risk that making an incident public will expose vulnerabilities before they can be remedied and that could endanger our systems and those in the core infrastructure of the internet.’

‘Depending on the scope of the reporting of incidents, we would be concerned over any potential reputational impact and associated costs.’

‘Penalties applied for avoidable breaches of security should be proportionate to the organisation's size and turnover. We note current criticism of the EU proposal to impose fines of up to 2% of global turnover for breach of data protection.’

‘If compliance to a set standard is enforced by regulations or legislation, then this may have the impact of reducing the best practice requirements for companies and member states that are well advanced in terms of Cyber security, whilst making it challenging for less advanced companies and member states to attain this standard. Sanctions will encourage litigation and as a result may increase costs to the organisations concerned, reduce the openness and encourage delays and obfuscation of detail needed by other organisations to analyse data and improve preparedness.’

‘…in certain situations an incident may require the intervention of law enforcement agencies. As such the public disclosure of the incident may damage any on-going investigation or raise the profile of the vulnerability before it has been effectively dealt with.’

CATEGORY N

That Member States encourage the use of standards and/or specifications relevant to network and information security

Summary

- Stakeholders raised concerns on how Member States would encourage the use of standards. If standards were encouraged on a national scale, this could lead to fragmentation in the market.
- While harmonised standards was seen by some stakeholder as a positive principle, views were also put across that this is a complex area and without appropriate industry engagement and development could be counter productive and stifle innovation.

Stakeholder Comments

‘Harmonised International standards implemented at a country level would be the most effective way of ensuring consistency of control and reporting … but would be a time consuming costly proposition before true benefits are achieved.’

‘We feel strongly that mandating standards in the information security area risks the creation of inappropriate one-size-fits-all requirements which would not be appropriate in the fast moving world of cyber security.’

‘There are references to standards and specifications but these are not defined which raises significant concern.’

‘Applying standards to critical infrastructures… can be helpful… standards compliance does not equal reduction in the number of incidents and complexity of events.’

‘Harmonisation of standards is highly desirable to create a way of working that is appropriate to the risks faced and how to deal with them.’

‘Cyber Security efforts are optimal when they reflect global standards and industry driven practices.’

‘…request that BIS recognises the value of British, European and international standards when considering how to encourage the use of standards to support this Directive and cyber security more broadly.’

‘Encouragement of the use of standards is a laudable principle but it must be recognised that requiring compliance to detailed technical standards by market operators is likely to be counter productive.’

‘We urge caution in specifying reporting requirements and standards at this stage lest it stifle innovation in the market.’

Conclusions and next steps

The Department for Business, Innovation and Skills is grateful for the wide range of responses that have been submitted in response to the Call for Evidence. We would like to thank the individuals, groups and organisations who have taken the time to contribute.

The UK shares the Commission's desire to improve levels of network and information security across the EU. We want to ensure that the internal market is a vibrant and safe place to do business and that Member States know who to contact in the case of a cyber incident and can effectively work together to reduce the threat and impact of cyber incidents.

The UK Government will negotiate at EU level for an instrument that does not overburden business, the public sector or other organisations; that encourages economic growth and innovation; and that fosters positive and sustainable behaviour change.

The negotiations in the Council of the EU, the European Parliament and the Commission are ongoing and will likely carry on into 2014. During this time, as new proposals and amendments are put forward, the UK Government may seek additional evidence from stakeholders and interested parties. Assuming the texts can be agreed by the European Parliament, the Council and the Commission, Member States, including the UK, will then need to consider how best to implement the legislation into domestic law. In addition, the UK Government will be required to complete a more in-depth Impact Assessment on the impact to the UK on the final proposal, should it reach this stage, as well as consulting on domestic implementation.

Consultation Co-ordinator contact details

If you have any comments or questions about the way this consultation was conducted you should contact the BIS Cyber Security Team at the following address:

cybersecurity@bis.gsi.gov.uk

Alternatively you may wish to write to the address below:

Department for Business, Innovation and Skills
BIS Cyber Security Team
Westminster
SW1H OET

ANNEX A

EU Cyber Security – An Opportunity for Businesses to have their say

22nd May 2013 – BIS Conference Centre

Summary of Group Discussions

This summary is based on the aggregated feedback from the six tables that took part in the discussion session.

Participants came from a range of sectors and roles including;

- Banking sector
- Financial Markets sector
- Energy Sector
- Transport sector
- Telecoms Sector
- Enablers of internet society providers
- Providers of cyber security
- Current regulatory bodies
- Policy Groups
- Trade Associations

The session was held under Chatham House Rules – comments are not attributed to any organisation that attended.

What should be the role of the EU in dealing with Cyber Security issues?

Participants agreed that Cyber Security was a global issue that required a coordinated response. The EU had capability to facilitate this and provide coordination both in the EU and to influence at a global level. However, Industry did not want to deal with a highly fragmented regulatory regime across multiple Member States – this fragmentation could also pose barriers to entry for new entrants. The importance of aligning the EU approach with that of other nations (such as the US) was also highlighted. The EU should be encouraging 'cross-border liaison and developing trusted exchanges'.

The EU role should not be heavy handed – focusing on education, raising awareness and promoting best practice – designed to both motivate and stimulate cyber security hygiene. It should also recognise the importance of activities at a national level. Attendees commented that different sectors had different requirements and that intervention should be done on a sector by sector basis and at a comprehensive level. There was also some discussion regarding the role the EU could play in stimulating the development and take up of standards – provided that these were risk based and specific.

Concerns were raised on the proposals of the NIS Directive – particularly on the burdens to organisations. Mandating incident reporting could stifle innovation and development of good cyber security practice (making it become a tick box exercise at its lowest denominator) and weaken the development of voluntary information sharing and trusted exchanges.

What kind of EU security breach reporting would your company be able to live with (if any)?

Significant concern was raised on the mandatory reporting requirements of the NIS Directive. Many participants indicated that they were not in favour of these proposals and that there were issues in the practicalities of implementing them.

Participants in regulated sectors said that in many cases they had an existing obligation to report breaches to their regulators and felt that this would add an additional reporting layer for a similar task. There were also concerns on how the NIS Directive would resolve itself with Data Protection regulation, and other existing requirements both at EU and national levels.

Fears were also raised that formal breach reporting could result in delays and that reported information would likely be crafted in a political/sensitive manner. Organisations would also bring in legal teams to the process to minimise risk liability on disclosure. There was a fear that compliance teams could be set up in place of more proactive cyber security teams to ensure a bottom line because it was mandated – cyber security would become a ‘stats game’. Genuine information sharing requires trust and mandatory reporting was unlikely to generate genuinely valuable data, simply compliance.

Information sharing and reporting (as long as the reporting was not mandatory) was however seen as potentially useful. Participants agreed they would benefit as long as the mechanism to report was easy to utilise, had appropriate levels of anonymity and that information only had to be reported once. In addition, many participants expressed the view that more should be done to improve capability proactively rather than focussing on reporting, which would do little to address the root cause of the problem and is like ‘shutting the door after the horse has bolted.’

Mandatory reporting potentially penalised those with better cyber security and reporting procedures in place as they would be required to disclose information that organisations operating at the minimum compliance level may not have detected.

There was significant concern on the capability for disclosures to remain safe and confidential the further information went up the reporting chain. There were also concerns that the measures would not be implemented evenly across the EU (the implementation of

Article 13 was cited as an example). Questions were also raised about what the Commission would do with the information reported to it, and how well protected it would be.

What kind of benefits/costs could the Directive bring about?

Participants agreed that defining specific costs and benefits was difficult at this stage without clearer definitions/thresholds.

There could be benefits from an overarching EU Cyber Security initiative – improved cyber capability in critical sectors; reduction to the costs of fraud to organisations; a more comprehensive collective defence. Greater information sharing could lead to an improved understanding on the origin of threats and potential patterns.

Some participants flagged that the Directive could have a negative impact on Cyber Security, stifling innovation and creating a compliance culture. They were opposed to the Directive on account that for additional costs to organisations, the measures would weaken current voluntary mechanisms in place with no additional benefit.

There would be costs related to the administration of the breach reporting; this would be more significant to smaller organisations with less available resources. Organisations would also be subject to audit, or potential fines should the competent authority deem them unfit to report on significant breaches. This in turn denotes a standard that organisations would need to conform to (which has not yet been defined).

While the UK is considered a champion in Cyber Security, there are many organisations, particularly those classed as SMEs, with minimal cyber security protection. While micro-enterprises are excluded from the Directive, it was important that these organisations be given the appropriate support develop their cyber security hygiene and capability. There was a concern that SMEs could shoulder a disproportionate burden to implement the Directive.

ANNEX B

UK comments on the European Commission's Impact Assessment on their proposal for a Directive on Network and Information Security

In general the European Commission's Impact Assessment provides a reasonable outline of the problems to be addressed and the potential reasons for the current underinvestment in security and resilience spending by the private sector. However, several questions on the issues remain and further clarifications on the following points would be helpful.

Market Operator Definitions

1. **Further clarifications around the market operators that will be subject to the NIS Directive will be essential as we progress through the negotiations** as there appear to be some discrepancies with respect to the sectors/ operators included. For example parts of the oil sector appear to be included in the list of sectors affected in the Directive document but not in the Impact Assessment.

2. **Further justification for why specific sectors have been included, in particular the enablers of information society services will also be essential to understand better the rational behind the Commission's selection**. For example, why have these sub sectors been chosen, and not hardware/software manufacturers?

Assessment of additional impacts

3. **A more developed assessment of significant impacts including social/employment impacts, competitiveness, data protection and international aspects would be useful**. This information would enable a greater analysis of the overall impact of the proposed Directive. In particular, it will be important to ensure that any proposed measures do not impact negatively on the operations of multinational companies who operate outside the EU, or mean that the EU is seen as a less attractive place in which to set up a business or from which to operate services.

4. We also believe that the Impact Assessment should consider and provide details on **potential unintended consequences of the proposal**. For example, an unintended consequence of the Directive could be that organisations may attempt to remain at a level classified as a micro business to avoid the additional regulatory burden. As we have already pointed out to the Commission, we also have serious concerns regarding the unintended consequences of breach reporting, and how this might act as a perverse incentive for businesses to improve their overall risk management practices.

5. We would also suggest that the development of a risk register associated with the measure would also help objectify potential consequences and risks.

Proportionality of imposing measures

6. The Impact Assessment does not provide sufficient analysis of potential costs and benefits that the measures will have across the wide spectrum of companies and organisations that could be affected. **Further breakdown would be welcome in particular on the impact of different groups, such as multinationals and SMEs.**

7. We would also welcome **further analysis of potential barriers to entry for new entrants to these sectors, and in particular consideration of the impact the proposals might have on innovation** in the sectors affected.

Cooperation between Member States

8. The Impact Assessment concludes that it is unlikely that all the Member States would reach comparable levels of national capabilities and preparedness via voluntary initiatives. This statement and the subsequent analysis provide a broad overview with the unsupported assumption that voluntary measures cannot coexist with regulation.

9. However, the UK Government suggests that **further analysis of the various issues that need to be resolved to achieve a comparable level of national capability and preparedness, with a comparison of the advantages and disadvantages of both a voluntary approach and a legislative approach would be invaluable. We would welcome further details from the Commission on why a voluntary (or a mixed voluntary/legislative) approach was not assessed in more detail.**

Key private entities and public administrations

10. The Impact Assessment does not analyse a voluntary approach for the private sector or public administrations, summarising the Problem Statement that there is insufficient business investment in security and lack of incentive to share information on NIS risk and incidents despite the worrying threat landscape.

11. We would welcome **more detailed analysis on how voluntary activities could play a role in enhancing EU wide capability in Network and Information Security.** As the Commission will be aware, the UK has so far achieved good results through voluntary initiatives which we believe could be negatively impacted by legislation. As above, we would stress that more detail on why a voluntary (or mixed voluntary/legislative approach) was not considered in more detail would be appreciated, especially due to the good results the voluntary approach is producing in the UK, and in other Member States.

Public Consultation

12. As part of the evidence gathering process for the Commission's Impact Assessment, an online public consultation ran from 23 July to 15 October 2012. A total of 180 responses were received.

13. A summary of the answers received for this consultation was included as part of the Impact Assessment. The information provided on the answers is however brief and **the UK Government would welcome further information on the consultation, both through a more detailed analysis (including potential biases for example through self-selection), and through publication of the responses to the consultation** (which the Commission had publicly stated would be made available following the consultation but have so far not been published.)

14. Examples of data that would be useful to understand from the consultation include **further breakdown of the statistics by sector, organisational size and geographical distribution of the figures cited in Annex 1 of the Impact Assessment.** Significant emphasis is given to the results from this consultation with respect to the selection of sectors that will be covered by the Directive as well as the arguments underpinning the preferred option chosen, and further analysis will provide clarity on the case put forward in the report.

Underinvestment in ICT security spending

15. The estimated figures for the natural growth of ICT security spending in 2012 is based on analysis carried out by Gartner. The single estimated figure of 8.4% provides no differentiation between the different sectors and we would welcome further information on how this figure was derived/ estimated and why it is appropriate to be used for all sectors. We have been unable to find the Gartner analysis in full.

16. We would also **welcome further information on why the energy sector's current investment is considered as a target for other sectors (as well as all company sizes within these sectors)**. Each sector has differing threats and risks and the security spending in that sector will represent those risks.

17. For example, **further clarity is needed on why healthcare providers will need to increase ICT security spending (as % of total ICT spending) to the same level as the energy sector. There is also no information that, while the Energy Sector is 'Best in Class' in regards to ICT security spending (as % of total ICT spending), that level of spending adequately meets a level of protection required for the Directive**.

18. These figures have a significant impact on the estimated compliance costs of ~1-2 billion euros.

Additional Costs

19. The report makes the assumption that only limited additional ICT security costs would be caused by the NIS Regulation. This assumption is based on the premise that the delegated acts will not substantially alter the current level of spending on Network and Information Security in the sector. Given that these delegated acts could substantially change the cost of implementing the Directive in the Member States, this then impacts the validity and range of the total cost figure for implementation as provided in the Impact Assessment (€1-2 billion.)

20. **We would welcome an update to the Impact Assessment once further information is available on where these thresholds could be set.**

21. An alternative method may be to estimate a potential threshold by looking at how the thresholds set for the Telecoms sector could be translated to the sectors covered by the Directive. This approach is being used for the UK Impact Assessment on the Directive.

22. We welcome the Commission's analysis of the cost of establishing a National CERT/Competent Authority in the Impact Assessment, and we hope that the requirements for such bodies do not become overly prescriptive in the regulation so that flexibility can be retained by Member States regarding how these bodies are constituted on a national level.

Overall Cost

23. While some analysis is provided on the assumption that between 40% - 70% of the additional required ICT security spending will not be caused by the NIS Directive, **we would welcome further information, including a more detailed breakdown on the relevant regulations that underpin this assumption. This is particularly important as the consultants (Gartner) state that reliable data on actual investment in NIS is hard to find.**

24. If the discounting is inaccurate or indeed variable across sectors and business size, then the cost to business will be significantly higher than the IA estimate. For example, the impact of this 'discounting' assumption (comparing Tables 12 & 13 in the IA) on the total cost to business is a reduction from €1.2bn to €539m (mid-point estimate). Applied to the Commission's estimate for cost per SME, this is a reduction from €8,333 (mid-point) to €3,750 (mid-point).

25. The Impact Assessment readily admits that 'continuous investment' in security measures will be necessary but is not clear on what the ongoing costs might be – largely on account of the difficulty of predicting technological change. This unknown cost is then 'offset' by the assumption that it will be outweighed by the assumed benefits of EU businesses cashing in on the 'global cyber security market'. **More detail on analysis of ongoing costs would therefore be welcomed.**

Summary

In summary, the specific questions and further detail we request of the Commission are as follows:

1. Further clarification of the market operators that will be subject to the Directive.
2. Further justification for why specific sectors have been included, in particular enablers of information society services.
3. A more developed assessment of significant impacts including social/employment impacts, competitiveness, data protection and international aspects.
4. More detail on the potential unintended consequences of the proposal
5. The development of a risk register associated with the measures.
6. Further breakdown of the impacts and benefits of the proposal on different groups, such as multinationals and SMEs.
7. Further analysis of potential barriers to entry for new entrants to these sectors, and in particular consideration of the impact for proposals might have on innovation in the sectors affected.
8. Further analysis of the various issues that need to be resolved to achieve a comparable level of national capability and preparedness, and a comparison of the advantages and disadvantages of both a voluntary and legislative approach.
9. Further detail on why a voluntary (or mixed voluntary/legislative approach) was not assessed in more detail.
10. A more detailed analysis of how voluntary activities could play a role in enhancing EU wider capability in Network and Information security.
11. Further analysis of the responses to the Commission's consultation, and publication of the responses.
12. Further breakdown of the data received in the consultation by sector, organisational size and geographical distribution of the figures cited in Annex 1 of the Impact Assessment.
13. Further information for why the energy sector's current investment is considered as a target for other sectors (as well as all company sizes within these sectors.)
14. Further clarity for why healthcare providers will need to increase ICT security spending (as % of total ICT spending) to the same level as the energy sector.
15. An update to the Impact Assessment once there are more details on where the thresholds will be set through delegated acts.
16. Further information, including a more detailed breakdown on the relevant regulations that underpin the assumption that between 40-70% of additional required ICT security spending will not be caused by the NIS Directive.
17. More detail on analysis of ongoing costs.

This publication available from www.gov.uk/bis

Any enquiries regarding this publication should be sent to:

Department for Business, Innovation and Skills
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000

If you require this publication in an alternative format, email enquiries@bis.gsi.gov.uk, or call 020 7215 5000.

BIS/13/1169