BIS | Department for Business Innovation & Skills

UK GOVERNMENT RESPONSE TO EUROPEAN COMMISSION CONSULTATION ON NETWORK AND INFORMATION SECURITY

OCTOBER 2012

Contents

Contents **2**
1. Introduction **3**
2. The UK approach to network and information security **4**
Government and Industry collaboration 4
Partnerships with Business to raise awareness of threats and mitigation and promote best practice 5
Focus on corporate governance 6
Focus on small businesses and individuals 6
Developing Standards 7
3. UK approach - Conclusion **7**
4. Where the EU could play a role **8**
Facilitating information sharing and supporting incident response 8
Improving capacity building through education and ENISA's activities 9
Promoting industry led security standards 9
Corporate Governance 9
A non-legislative sector specific approach 9
Building confidence in the digital single market 10
Supporting Research and Development and growing the cyber security sector 10
5. UK concerns regarding a regulatory approach **10**
Sector by sector approach 10
Incentives and compliance 11
Definition of incidents and sectors 12
Regulatory burdens on business 12
Cost to the public sector 13
6. Other comments **13**
CERTS 13
Information sharing 14
Wider Commission/EEAS strategy 14
Annex A **15**
The Energy Sector 15
The Finance Sector 15
The Health Sector 16
The Transport Sector 16
Annex B **18**
Response by the UK Government CERT/CSIRT community to the EU Public Consultation on improving NIS in the EU **18**
UK Current Situation 18
International CERT Co-operation 19
ENISA 19
CERT-EU 19
Inter-CERT Cooperation 19
Data sharing across the CERT Community 20

1. Introduction

The UK government welcomes the Commission's desire to seek improvements in the area of network and information security across the EU. The need to improve network and information security within, across and beyond Europe is clearly a vitally important objective for businesses, individuals and the wider economy. The UK is very active domestically in this area and we are also keen to engage fully at EU and international level on these issues, and to share our experience. In this response to the European Commission's consultation on how to improve Network and Information Security in the EU, we set out the UK's approach to the issues, and explain where we believe the Commission could play an important role.

The UK Government has been clear that every sector of society – Government, business, the public, and law enforcement – has a part to play in helping to protect the UK from cyber threats. A major part of this approach is the Government's ambition to encourage information sharing within and between sectors to help mitigate these threats. The UK is approaching issues of network and information security from a non regulatory perspective whilst also using existing regulatory measures on a sector specific and targeted basis.

The UK believes that it is of primary importance to raise awareness and identify and assess risks to allow effective mitigation to be put in place. There are a range of options for achieving this, and before further legislation is considered, both at a national and EU level, it will be important to understand whether such legislation would be more effective in delivering these outcomes than other options. Where the UK Government has been persuaded of the necessity of regulatory measures for some sector-specific and targeted measures then it has taken that approach. However, in the first instance, it remains our objective to reduce unnecessary regulation of businesses and seek to pursue voluntary and cooperative arrangements wherever possible.

We therefore have some concerns surrounding the Commission's desire to introduce legislation in this area, when we believe that other options should be considered first. We have particular concerns regarding the proposal to extend mandatory security breach disclosure to other sectors, since we believe that legislation will penalise those businesses who are mature enough to detect breaches, and will not create the incentives to implement more holistic behavioural change for those companies at the lower end of the cyber maturity scale.

Fundamentally we believe that cyber security should be seen as a driver or enabler for growth, not as an end in itself. As such, the UK would not support legislative proposals that are aimed at enhancing cyber security but which stifle the possibilities for economic growth or have the potential for unintended consequences.

2. The UK approach to network and information security

The UK considers cyber security as a top priority. The UK has published a National Cyber Security Strategy and put in place a dedicated national cyber security programme to deliver the strategy. The objectives of our national cyber security strategy are:

1. The UK to tackle cyber crime and be one of the most secure places in the world to do business in cyberspace.
2. The UK to be more resilient to cyber attacks and better able to protect our interests in cyberspace.
3. The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies.
4. The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives.

The UK government is very active in considering the issues in this area and working with businesses in order to improve levels of network and information security. We are pursuing non regulatory approaches to support and incentivise businesses and consumers to take action, rather than imposing regulation before businesses have been given the guidance needed and the opportunity to raise their capabilities. Our approach is characterised by far-reaching cooperation and collaboration between government and the private sector. Key measures we are promoting in particular include:

- Partnerships with business to raise awareness of threats and mitigation
- Ensuring cyber security is part of corporate governance best practice
- Awareness raising with small businesses and individuals
- Developing standards to enhance – and inform – relative levels of cyber security.
- Improved reporting of cybercrime to law enforcement, and greater sharing of alerts with businesses and individuals.
- Developing innovative collaboration environments in partnership with industry to facilitate real-time information sharing.

Although we are still in the initial stages of progressing some of this work, we are confident that these measures are a productive initial step in encouraging both industry and individuals to take greater consideration of the risks posed by cyber threats, as well as to help them learn how to mitigate these risks. More detail of each area of this work is set out below.

Government and Industry collaboration

The UK government recently piloted a collaborative initiative between government and industry to help reduce the vulnerability of the UK to cyber attack. The project aimed to catalyse the development of capability to counter cyber threats through facilitating the sharing of cyber attack information across a range of groups including:

- within industry sectors
- between industry sectors
- between industry and Government
- between industry and law enforcement

The Pilot (concluded in March 2012) demonstrated that industry could share information, knowledge and experience for mutual benefit across sectors. Government and industry partners are now actively working to create a scalable and sustainable collaborative operating environment to build on the current momentum and demonstrate enduring value and benefit to the project's community of stakeholders.

We are also actively exploring the incentives businesses need to share information. It has become clear that businesses go much further than base level compliance exercises in terms of strategy, commitment, analysis and learning when they share information in a non-regulatory and 'safe' environment, where they are able to benchmark their cyber security maturity against others and receive useful information, both from other businesses, as well as information from government and law enforcement bodies on threats and mitigation.

A key benefit of the collaboration environment will be the analytical function that will digest and process the information that the participants feed in. This will enable participants to receive direct and relevant advice on specific threats from the central function, in addition to direct information from other participants.

The project is being run jointly with industry partners, and the participation criteria, operating model and building of the actual environment is a collaborative venture. We intend to go live with the new environment early in 2013.

Partnerships with Business to raise awareness of threats and mitigation and promote best practice

The UK government is currently working with several sectors (including Professional Business Services, ISPs, Universities, Life Sciences and Retail). Companies across these sectors display a broad range of cyber security maturity. The aim of this work is for government and industry to discuss issues together in order to raise awareness across the sector base and explore how sectors can better protect themselves. Discussions are not restricted to technical risk mitigants, and include information management, human vulnerabilities and corporate risk framework. The partnerships will draw on the support of key trade associations, training bodies, HMG expertise and individual companies with higher levels of cyber maturity.

This work aims to consider the cyber threat in the round, not merely from a high level, or technical point of view. We expect that this work will ensure that both government and industry are aware of the range of areas which can be engaged in order to improve risk management of cyber threats. This work should also help raise awareness of issues in sectors which may not currently have the appropriate risk management practices in place.

Specific work is also ongoing between Government and law enforcement bodies in partnership with ISPs with an aim of improving the online security of their customers through raising awareness and increased collaboration between ISPs and law enforcement bodies.

More broadly, there is activity underway across the UK government to raise awareness of the threats and provide advice. Guidance for companies is available on the CPNI website (cpni.gov.uk) which lists 20 critical controls for effective cyber defence, along with a comprehensive range of physical and personnel protective measures. CPNI also facilitates 'information exchanges' within sectors which allow one company to learn from the experiences, mistakes and successes of another, without fear of exposing company sensitivities. These

information exchanges are greatly valued by the participating sectors, and this idea has also been exported to other countries.

Focus on corporate governance

The UK government believes that the cyber threats facing businesses and their supply chains today will not be solved through investment in technology alone, but through concerted risk assessment which culminates in businesses identifying what critical information assets need prioritising – and in the establishment of a cyber risk oversight governance structure managed at Board level. This process should certainly include security and technology personnel, but we believe that the Board should be firmly in charge. The UK Government has established strong working relationships with a number of influential professional, representative and training bodies (e.g. risk, audit, etc) and will be working closely with them to raise awareness and encourage a risk assessment approach to mitigating cyber risks. These interactions will result more informed discussion in the board room.

We have also recently published a Cyber Security Guidance Booklet for Business. The Cyber Security Guidance pulls together Government expertise in an accessible toolkit to support businesses in dealing with the growing cyber security threat. The Guidance is targeted at board level and designed to offer some practical steps which companies can take to improve the protection of their business assets from technical, commercial, and financial threats. A copy of the Booklet can be found at http://www.bis.gov.uk/policies/business-sectors/cyber-security/downloads. We hope that this free and accessible guidance will play a significant role in incentivising business to manage the cyber security risk as a corporate risk under direction from the board.

The UK government is also working closely with the Financial Reporting Council on the review of the UK Corporate Governance Code and associated risk guidance. There is widespread recognition that the guidance should reflect a more contemporary threat landscape.

Focus on small businesses and individuals

Get Safe Online in the UK are working closely with Government to increase cyber security and awareness in SMEs. This work is also underpinned by research undertaken with the National Fraud Authority.

Get Safe Online is a public/private partnership combining the resource, ideas and actions of a small team supported by organisations from law enforcement, the public and commercial sectors. Their activity is twofold: to create and manage year round campaigns driving awareness and education around enjoying a safe and secure online experience for SMEs and individuals, and managing and maintaining their destination portal – www.getsafeonline.org – as a dynamic and effective provider of substance on online security.

The organisation ensures that the needs of both the public and private sectors are recognised when deciding on the best way to raise awareness and improve online security practices in small businesses. The Get Safe Online steering group which is made up of public and private sector partners works towards devising approaches to address to key findings of their primary research – such as the strong appetite from small businesses for an objective, independent voice and advice on online security issues and the absence of scaremongering to promote an entirely constructive online experience.

There are a number of events running throughout the GetSafeOnline year. One focus is the GetSafeOnline week in October – in 2012 on the theme 'click & tell'. Following through the positive approach, they are conducting a five city roadshow across the UK of campaign and communication offering drop in centres in key public places (e.g. train stations) where consumers and small businesses can ask an expert for good counsel on online safety. The campaign theme encourages consumers and businesses to tell a friend or colleague a piece of advice on online safety, and then record that on the website to share with the GetSafeOnline community. Get Safe Online anticipates a best ever reach for this year's week, in excess of 16m – all based on the premise of enabling consumers and small businesses to enjoy their online experiences in a safe and secure way.

Developing Standards

Standards are a key enabler for delivering the objectives set out in the UK's Cyber Security Strategy. But this is a complex environment that cuts across public sector and private sector and has both a national and international dimension. Detailed activity is at an early stage but the key work streams in this area include:

- Establishing a map of the cyber security standards landscape in order to undertake a gap analysis and better inform requirements;
- Exploring the potential to develop new cyber security standards - working with international standards bodies where appropriate;
- Helping to foster the development of industry-led standards – and exploring the benefits of creating an overarching mechanism for users to recognise what a 'good' scheme or standard looks like;
- Supporting the development of commercial service offerings which can help companies to assess their level of cyber security.

Other activity such as the ongoing role that the UK Government undertakes in providing assurance and certification for certain products, services, people and organisations will complement this work.

3. UK approach - Conclusion

In addition to the initiatives described above, there are also regulatory measures in place in the UK, derived both from domestic and EU regulation, as well as guidance which provides security and resilience advice for certain sectors.

Many sectors in the UK already have specific obligations which require them to report and respond to incidents of cyber origin, and from other sources (see Annex A for further details.) We believe that these different measures also reflect the fact that it is important to consider each sector individually, due to the fact that each sector faces different risks, and the impact of these risks can differ significantly from sector to sector, as well as within sectors. As a result, we believe that the risks of each sector require a tailored risk mitigation response, as opposed to a one-sized-fits-all approach.

As can be seen from the detail set out above, the UK is approaching the issues of network and information security from a non regulatory perspective whilst also utilising existing regulatory measures on a sector specific and targeted basis.

The UK believes that it is of primary importance to raise awareness and identify and assess risks to allow effective mitigation to be put in place before legislation is imposed. As is demonstrated by the work we are carrying out in the UK, there are a range of possible options for achieving awareness raising and risk mitigation. Before further legislation is considered, both at a national or EU level, we believe it is important to understand whether any such legislation would be more effective in delivering these outcomes than other options. Where the UK Government has been persuaded of the necessity of regulatory measures for some sector-specific and targeted measures then it has taken that approach. However, in the first instance, it remains our primary objective to reduce unnecessary regulation of businesses and seek to pursue voluntary and cooperative arrangements wherever possible.

We believe the advantages of our non regulatory approach are as follows:

- Allows business to improve capability and develop their risk management practices.
- Focuses on building trust and the benefits of sharing information, rather than on compliance and potential punishment for mistakes.
- Focuses on preparedness and prevention rather than addressing the issue after the event.
- Gives government the role of promoting and facilitating, but recognises that industry and business have responsibilities themselves to provide effective security.
- Takes into account incentives for businesses to act and fosters a pro-active culture.
- Takes into account the current economic situation and national and EU commitments to reducing regulation.

Our strategy will be assessed on an ongoing basis to evaluate its impact. The UK does not rule out the possibility of adopting a regulatory approach in the future should the evidence suggest that this is needed, however we believe that we need more information about the impact and benefits of different options before we consider regulation.

4. Where the EU could play a role

We believe that the EU does have a role to play in network and information security, in particular in supporting Member States to raise their capacity and capability as well as ensuring a more cohesive EU approach to cyber issues. The Commission should however recognise those areas where Member States have competence and where action is best achieved on a national level, as well as ensuring that non regulatory options are considered before any legislation is adopted.

Areas in which we believe the EU has competence and could play a useful role are as follows:

Facilitating information sharing and supporting incident response

The Commission could play a useful role in encouraging MS to share information on best practice and in providing assistance to MS (through ENISA for example) to reach appropriate levels of cyber security. Encouraging all MS to reach a consistent level of cyber security will be important in order for MS to be able to feel confident in sharing information with each other.

However, the UK would argue that the Commission should not oblige MS to share information with each other, or dictate what type of information should be shared. Due to national security considerations and the need for *effective* information sharing to be predicated on trust rather than legislative requirements, MS should retain the power to decide what type of information is relevant. We would also expect that the Commission and ENISA would not be able to access such data until their own systems are more secure than at present. In addition, building a pan-EU secure system to facilitate such information sharing would be a very challenging task.

The Commission could also play a useful role in collating a directory of points of contact and creating links between MS. Organising and promoting cyber exercises should also be continued, and is a key part of ensuring adequate incident response mechanisms are in place

Improving capacity building through education and ENISA's activities

ENISA plays a key role in raising awareness in MS and helping build capacity. This role should continue, and ENISA should be directly involved in contributing to the Commission's policy proposals in this area due to their expertise. ENISA also has a key role to play in liaising not only with MS governments, but also with CERTs and groups responsible for promoting awareness and best practice to individuals, as well as businesses. It will be important however for ENISA to remain as an advocate to MS, and not to take over responsibility for tasks that MS should be encouraged to carry out themselves. We would also want to ensure that ENISA and other EU bodies, in particular the newly created European Cyber Crime Centre work together in a complementary manner to ensure that work is not duplicated.

Promoting industry led security standards

The Commission could play a role in supporting MS work on standards. The Commission could perhaps also contribute to work on creating a pan – EU industry standard for cyber hygiene. A common standard or mapping of federated MS policies will enable trust through consistent management, protection and decision making regarding sharing information between MS. Any standards which are promoted should however be reviewed on a frequent basis to ensure they are up to date and reflect current threats.

Corporate Governance

The Commission could also consider ways of working with Member States to encourage businesses to take adequate consideration of the threats posed by cyber risks at a Board level, such as through providing guidance on how best to produce a Board level strategy which deals with risk assessment and key challenges, and practical measures for dealing with cyber issues as a long term corporate risk.

A non-legislative sector specific approach

The Commission could also set out high level objectives for levels of cyber security in each sector and work closely with other DGs in order to ensure that each sector is adequately addressing cyber risks in its existing work. This could be achieved through an initial focus on benchmarking capabilities in order to establish specific areas which need to be addressed. This would ensure that existing EU measures and regulations are taken into account, and that

consideration of cyber threats, response and mitigation is fed in to the development of non legislative sector specific initiatives.

Building confidence in the digital single market

The Commission has a key role to play in establishing the digital single market and ensuring it functions fully. The Commission, along with ENISA, can play an important role in ensuring that businesses and customers know how to protect themselves online, and are confident in conducting business on the internet in a responsible manner.

Supporting Research and Development and growing the cyber security sector

As part of the wider Horizon 2020 agenda, the Commission has a vital role to play in making the EU a hub for innovation. Encouraging research and development into the cyber security sector and using Horizon 2020 funding to support this would be welcome.

5. UK concerns regarding a regulatory approach

As is clear from the work we are undertaking in the UK, we believe that there are a range of non regulatory measures which should be considered before resorting to regulation in this area. Before regulation is considered we would need to ensure that there is a detailed understanding of desired outcomes, and be confident that legislation would be more effective in achieving these outcomes than other approaches. It will also be important to ensure that any legislation does not introduce unintended consequences. Our particular concerns regarding the Commission's current proposed regulatory approach are set out below.

Sector by sector approach

As demonstrated in our comments on existing sectoral regulation and guidance in the UK, we do not believe that a 'one size fits all' approach to cyber security in all sectors is a proportionate or necessary response to the issues identified. The risks and consequences of cyber attack in each sector are different, and should be mitigated accordingly. For example, the sectoral approach to our Critical National Infrastructure was developed through examining each sector individually and different criteria and measures were found to be appropriate.

As we point out above, there are already provisions in place in some sectors for security and resilience which respect the individualities of each sector and which have taken into account the views of stakeholders in that sector. Although we understand the Commission's desire to ensure there is a comprehensive approach to network and information security, we do not feel that existing measures and the differences of each sector have been appropriately taken into account in the Commission's proposals to date. We set out what we consider the Commission's role could be above, such as introducing high level guidelines or standards, encouraging a greater focus on cyber threats at a more senior level, as well as looking at the issues on a sector by sector basis.

Whatever measures the Commission chooses to bring forward, it will be important to consult widely internally with DGs relevant for each sector in order to ensure a comprehensive understanding of measures already in place, or intended in the future for each sector.

Incentives and compliance

We are not convinced that regulatory measures which make security breach disclosures mandatory would provide business with the right incentives to disclose information or to improve existing cyber security measures. At present, we believe that businesses require guidance and encouragement to look for issues and address them, rather than penalties for issues which they may not have the capabilities to address.

Paradoxically, the introduction of mandatory security breach reporting could mean that those who are better capable of finding and reporting security breaches are penalised, when in fact they should be the ones who are being rewarded for their good practice. Making security breach disclosure mandatory is therefore likely to discourage businesses from improving their cyber security practices and actively looking for threats, and would therefore be a disincentive to addressing cyber risks. The reputational damage and cost to business that disclosing breaches entails is also likely to be a disincentive to disclosure. Studies have confirmed these negative effects where breaches of confidentiality caused a decline in the company's market value of 5% on average or it lost 2.1% on average of the stock market value within 2 days of the breach being announced[1]. Although a short time affect on a company's market value may lead to more long term savings through actions taken after the event, we consider that in the current economic climate businesses are unlikely to be willing to risk reputational and financial damage, and will therefore avoid public reporting any more than is strictly necessary.

Although it could be argued that this avoidance of reporting to prevent reputational damage is precisely the reason why reporting should be made mandatory, we believe that the perverse incentives mandatory reporting could lead to outweigh the benefits it might bring. Although mandatory reporting might see an increase in reports produced, businesses have informed us that it would effectively put an end to a cooperative, sharing relationship between businesses and government, and would deprive businesses of the means through which they can share information on a trusted basis, instead changing this to a legal requirement which must be complied with. The view of a number of major UK companies we have spoken to suggests that introduction of regulation in this space is likely to mean that companies put in place the minimum measures necessary to achieve compliance with the law, and in general will not look to go beyond this in order to achieve more full scale and effective behavioural change. Businesses would be much more willing to share information on a trusted 'no blame' basis, where they can see that the information they are providing is helping towards improving security and addressing crime. On the contrary, businesses would be much less inclined to carry out reporting where they see no evidence of the benefits of their reporting.

Whereas mandatory reporting might see a short term improvement in the number of reports produced, the UK believes that a non regulatory approach achieves more open and transparent engagement between businesses and government as businesses feel more inclined to engage in a non regulatory environment where there are fewer legal risks and more flexibility and

---

[1] Campbell, K, et al, 2003, The economic cost of publicly announced information security breaches: Empirical evidence from the stock market, Journal of Computer Security 11 (3) pp. 431 -448 and Cavusoglu, H, Mishra, B. and Raghunathan, S, 2004, The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers, International Journal of Electronic Commerce, 9(1) p. 69

opportunity to be cooperative. Our ambition is that the work we are undertaking as part of our Cyber Security Strategy to raise awareness with businesses through non regulatory measures will create more effective and holistic behavioural change than regulation in this area could achieve. Our work with business so far has led us to believe that a non regulatory approach creates more incentives to change behaviours than a regulatory approach, which although it may force a response, often does not change behaviours for the better and in this case we believe could actively discourage businesses from addressing their network and security issues.

We believe that it is therefore important to ensure that education, awareness raising and capability building are introduced, and the impact of these measures assessed, before considering regulatory measures which effectively punish companies for security incidents before they have the correct resources in place to deal with such incidents.

Definition of incidents and sectors

We also have concerns regarding how a cyber security breach should be defined in order to drive an appropriate – and positive – result. For example, many criminals attack networks through third parties, such as customers or partner organisations, so a network could be attacked and harm caused without actually being breached itself. A more holistic and high level approach focussing on capabilities would therefore be more appropriate than asking businesses to report breaches, when breaches which affect them often occur outside of their networks. Businesses should be incentivised to look for breaches to their networks as well as working with their partners to do the same to achieve a high level of cyber hygiene for all. A focus on corporate governance and the management of long term risks is, we believe, far more likely to achieve a solution to this issue than asking businesses to report breaches after they have occurred.

The Commission should also ensure that the scope of any sectors on which regulation is imposed is well defined. For example, in the UK the finance sector consists of a broad and diverse set of institutions, not all of which are regulated. Introducing regulation across the sector as whole would therefore be an extremely difficult regulatory challenge. It is also important to take into account the fact that many large businesses are multinational organisations, and are therefore dealing with a range of legislation not only within the EU but globally and are reluctant to see further legislation in this area.

Regulatory burdens on business

In the current economic climate the Commission should not be imposing more regulatory costs on businesses unless there is no credible alternative to regulation. This would run counter to the Commission's and many Member States' domestic efforts to reduce the burden on business of unnecessary regulation, and to the EU's wider efforts to promote growth (as set out in the clear objectives of the Compact for Growth and Jobs, agreed at the June European Council.) As set out above, the UK has already adopted a non-regulatory approach to network and information security across several sectors. We feel that any EU-wide action in this area should consider adopting and, if necessary strengthening, existing non-regulatory good practice. If regulation is considered necessary, this should be accompanied by a robust analysis of the impact on business, including costs and benefits, that has received a positive opinion from the Commission's Impact Assessment Board. This should be informed by detailed consultation with businesses and especially small businesses.

A proposal for a regulation should comply with the Commission's commitment to exempt micro businesses from new EU legislation unless there is a compelling reason to include them, and to

develop lighter regimes for SMEs more generally. Consultation with businesses will be crucial to the development of an approach that avoids disproportionate impact on SMEs. Although we welcome this consultation, we have received evidence that many businesses are unwilling to respond due to the sensitive nature of the questions posed, and the fact that many businesses do not wish to reveal details of security breaches they have suffered in public (even if the response is anonymous.) We therefore feel that the Commission could do more to engage with businesses on this issue, and should consider issuing another consultation once proposals are more firmly established in order to give businesses more detail on which to base their responses. A further consultation on detail of any proposal could achieve greater clarity regarding the financial impact any regulation may pose, without asking businesses to reveal incidents which have affected them.

Cost to the public sector

At a time when Member States' budgets are under pressure, we have concerns regarding the extra cost that mandatory security breach reporting would impose on regulators. Some regulators may not currently have the capacity to deal with and enforce reporting, or may have to enforce new measures which are very similar to other measures in place or about to be introduced (i.e. data breach reporting). We would also encourage the Commission to consider the fact that there is already a significant amount of security legislation in place (Article 13a, Art4 of the e-Privacy directive, the proposed amendments to the Data Protection regulation, and the measures contained in the E-signatures and E-Identification regulation.) We would strongly suggest that all breach notification measures should be considered in the round, as adding further security related measures will significantly add to the already high burden imposed on regulators, and lead to a situation where reporting on such a range of regulations may become unrealistic.

It will also be necessary to consider whether the threat and risk assessment justifies a regulatory approach. In addition, we are unclear as to how mandatory security breach reporting would be carried out in currently unregulated sectors, such as e-commerce businesses, as well as in sectors such as finance where there is more than one regulator in the UK, and also parts which are also unregulated. We would also be concerned if the proposed 'competent authority' in each MS had to deal with security breach notifications from all sectors, as this would be an extremely difficult job, and would require additional levels of resource which are not currently available. Should the Commission decide to bring forward regulation, we would therefore expect the cost to government to be carefully evaluated in the impact assessment.

6. Other comments

We also have some comments on the following issues that the Commission are considering acting upon:

CERTS

The UK agrees with the concept of setting up a national competent authority in order to be a point of contact for cyber incidents and to share information. However we would have some concerns about the Commission setting out detailed parameters for the CERT landscape within Member States. The UK considers the design of our CERT landscape to be a national competence, and would therefore not be content with the Commission setting out in detail what it

should look like. Annex B provides a technical response from the UK CERT community which addresses these issues in more detail.

Information sharing

We have concerns regarding the Commission's intentions to mandate Member States to share information with each other and with the Commission. We believe that it is important to build trust before sensitive information is shared, and would not be willing to do so if we were not fully confident in the body receiving sensitive information. We believe that the Commission's role in this area should be to *facilitate* information sharing between MS, and to encourage capability building. We do not believe that *mandating* information sharing, or setting out what type of information MS must share will be the most effective way in which to improve sharing of threat information and incident response.

Wider Commission/EEAS strategy

We welcome the Commission's desire to work together with the External Action Service to take a broad approach which focuses on the economic and social benefits of cyberspace, not just cyber security. We believe that the strategy should set the context for current and future EU initiatives and activities on cyber, and that there is large potential for the EU to spread good practice and interoperability. The EU also has the potential to maximise MS' collective impact internationally, however the EU's policies should at all times remain consistent with the principles of the Lisbon Treaty, especially those of subsidiarity and proportionality which are extremely relevant when working in an area which risks impinging on issues of national security. Ongoing consultation of MS on all cyber issues is therefore welcomed, and we look forward to working closely with the Commission in the future.

Annex A

Many sectors in the UK already have specific obligations which require them to report and respond to incidents of cyber origin, and from other sources. We focus on the energy, finance, transport and health sectors below due to the Commission's stated interest in applying regulatory measures specifically to these sectors. Due to the fact that elements of these sectors are part of the critical national infrastructure, there will be some sensitivities regarding security information which they divulge and differences between how these sectors are approached in comparison with others.

We should also point out that in many sectors, and specifically in the transport and energy sectors, there is a strong correlation between safety and security, and the two are often inextricably linked. Measures in place which are aimed at increasing safety should also be taken into account when looking at security measures, since they may often achieve the same outcome.

The Energy Sector

In the UK, Regulation 32 of the Electricity, Safety, Quality and Continuity Regulations 2002 ensures that the following interruptions to electricity supply are reported to the Secretary of State:

- Interruptions of 20MW or more for three minutes or longer.
- Interruptions of 5MW or more for one hour or longer.
- Interruptions of 5000 consumers or more for one hour or longer.

Energy companies also report interruption data to the regulator, Ofgem, as part of a reliability incentive scheme. These measures are aimed to ensure that the public receives a consistent supply of electricity, and that any divergence from this is reported.

In the nuclear electricity generating area, there are many security measures in place nationally (principally through the Office for Nuclear Regulation) to protect systems which could be subject to cyber attack, taking into account international standards in this area.

The Finance Sector

The finance sector in the UK is extremely diverse, with several measures in place in this area. Reporting requirements on firms are covered at a domestic level by the Financial Services Authority (FSA) in the FSA Handbook under the "Principles for Businesses." Principle 11 of the Handbook states that "A firm must deal with its regulators in an open and cooperative way, and must disclose to the FSA appropriately anything relating to the firm of which the FSA would reasonably expect notice." This is a legal requirement set out in secondary legislation, which means that any incidents (including cyber incidents) which affect a firms business or clients must be reported to the FSA. The Handbook contains further specifications which provide more detail regarding how the reporting should be undertaken.

In addition, the Bank of England's Bank Oversight Team would expect to receive reports on payment scheme breaches or outages from the banks themselves. Reporting of particular

events by payment systems to the BoE are made under the 2009 Banking Act and the 1999 Financial Markets and Insolvency (settlement finality) Regulations.

Work is also ongoing through a 'Virtual Task Force' model, which is currently established through voluntary participation of key organisations in the private financial sector. Private institutions are working with law enforcement to respond effectively to threats to the financial sector. There have been a number of major operations by the Police Central e-Crime Unit resulting from this engagement, resulting in the arrest of a large number of individuals and the disruption and prevention of a significant level of financial crime.

It should also be noted that the finance sector consists of a broad and diverse set of institutions, not all of which are regulated. Introducing regulation across the sector as a whole would therefore be an extremely difficult regulatory challenge.

The Health Sector

In the UK there are no legislative requirements to report security breaches in the health sector. However due to the sensitive nature of information held by the sector, data losses are taken extremely seriously. There is a requirement through internal procedures and guidance for personal data losses in the National Health Service (NHS) to be reported centrally to the Department of Health if they meet requirements which define them as being above a certain level of seriousness. NHS organisations must also inform the Information Commissioner's Office (ICO) of serious data losses. Many organisations also report lower levels of data loss or unauthorised disclosure incidents to the ICO, and the Department of Health regularly meets with ICO officials to discuss NHS data loss incidents and progress.

The NHS also has internal reporting mechanisms for security issues, and issues guidance on best practice and ISO standards. The existing information governance incident reporting arrangements are continually reviewed in light of evolving security developments.

Organisations which require access to NHS infrastructure, national services and others that access or process patient data must satisfy published NHS Information Governance (IG) standards. For new organisations, this involves a formal IG statement of compliance and acceptance of conditions for provisions and use. For all organisations, an annual IG toolkit attainment report is required against published requirements including network security.

The Transport Sector

In the UK there are threat-informed and risk-based Counter Terrorism regimes in place for land, maritime and aviation. Work is underway to understand potential cyber issues specifically in areas such as Air Traffic Control and rail command and control systems. Of course there is regulation in place across all transport modes covering safety but this does not specifically address malicious interference with electronic systems. The Department for Transport (DfT) and CPNI are working to encourage the transport sector to take cyber security issues more seriously to ensure that they are sufficiently aware of vulnerabilities, can act to minimise risk and react to mitigate the effects of attacks that do occur.

DfT currently considers that guidance to industry is most likely needed in future. Targeted regulation may also be, needed, but it is too early to tell exactly which will be the best approach.

There are also many measures regarding security and safety in the transport sector in place across the EU and internationally. In particular DGHome and DGMove have responsibilities and are carrying out ongoing work with the likes of IntCen to evaluate threats and risks to the aviation sector and to regulate accordingly.

The UK believes that the different approaches to security in these sectors must be taken into account when considering a regulation which affects them all. As is demonstrated above, each sector has different ways of dealing with security incidents, whether cyber specific or not, and this reflects the different priorities and risks in these sectors. We strongly believe that existing guidance and legislation, both at a domestic and EU level must be taken into account before imposing new security legislation on these sectors.

Annex B

Response by the UK Government CERT/CSIRT community to the EU Public Consultation on improving NIS in the EU

UK Current Situation

The UK Government gives a very high priority to operational cyber defence and believes strongly that an effective CERT network is an essential tool against the threats from cyberspace, which are numerous and serious. It should be noted that all CERTs are different. Each has its own communities, responsibilities, capabilities, funding models and services. http://www.cert.org/csirts/services.html

We believe that each EU MS should design and operate its government CERT network according to the needs and structures of that MS. The result of that design should be measured by the effectiveness of the service provided by those CERTs, although existing government structures may have to be allowed for. In the UK there are currently 3 government CERTs :-

- CSIRTUK focussing on support to the UK's CNI
- GovCertUK focussing on support for UK Government networks
- MODCert with a specialist role focussing on support to military networks

This structure has been adjusted several times in the face of operational needs, and whereas the 3 organisational structures are independent, there is a great deal of joint working, staff interchange, formal and informal cooperation. All 3 CERTS exist at the heart of the UK national security structures and there are very few externally-imposed restrictions on data sharing between them.

There are a number of non-government CERTS in the UK as well.

There has been discussion in the UK about having a National CERT. Currently, there is no UK National CERT. There are CERTs for particular sets of customers which have national responsibilities within their own communities (CSIRTUK and GovCertUK are examples) but no single CERT which has overarching national responsibilities and to which other CERTS are subordinate. This issue has been discussed many times in the UK, and the subject is kept under review. If the UK chooses to establish a national CERT, then that CERT is likely to be structured to suit the UK's circumstances, so as to provide the best possible service to customers.

We also note the value of WARPs[2], and believe that for some communities these represent the best way forward

International CERT Co-operation

It is clear that the threats are international in nature, and cross-border action is a very important aspect of network defence. We work jointly with other nations, and we encourage all nations to establish and operate effective CERTs, although we respect the fact that other nations will have different CERT structures compared to that of the UK. The value we place on a CERT partner is likely to be influenced by factors such as the ability to establish **trust**, the **expertise** of the CERT, and the **capacity** to work with us. Whereas there are global CERT organisations (eg FIRST) it is generally easier to develop trust within regional groupings, where regular contact is a key factor. Clearly EU developments are of huge significance to us and we are pleased to have the opportunity to contribute to the consultation.

Whereas CERTs are key elements in incident response, both GovCertUK and CSIRTUK are part of larger organisations which have security as central to their mandates, and those organisations are part of schemes for escalating incidents on a national basis, so that serious incidents can be handled nationally and internationally by the most appropriate channels available, including a variety of inter-governmental and multi-lateral channels.

ENISA

Particularly on the expertise aspect, we see a very important role for ENISA in gathering, analysing and disseminating Best Practice related to CERTs and network security. ENISA has a vital task in helping European CERTs to develop up to the best possible standard, and in assisting nations to set up government/national CERTs if they have not done so yet. We believe that the skills and capacity of ENISA are best used in this way and that ENISA's mandate should not expand into an operational role.

CERT-EU

We wish the CERT for the EU institutions to flourish and develop into a very effective body giving the best possible support to those institutions. As it becomes fully established, we expect to develop a good relationship with CERT-EU.

Inter-CERT Cooperation

We believe that inter-CERT cooperation is essential. Such co-operation has routinely developed along both bilateral and multilateral lines already among a number of EU government CERTs, and this process should be encouraged. In a fast-moving incident response environment, trust and familiarity with partners is a key factor in information exchange.

We note that EGC, an entirely voluntary and self-regulating body, has become a very effective forum for exchange between members. However EU inter-CERT forums develop in the future, we do not wish to lose the benefits delivered by EGC, or to lose the contribution from the non-EU members of EGC. There are precedents for European nations (especially those with a

[2] Warning, Advice & Reporting Points www.warp.gov.uk

Security Agreement with the EU) not in the EU to contribute on EU security subjects, the GALILEO project for example.

Data sharing across the CERT Community

There has been discussion about mandatory data sharing of cyber incidents across the EU, and some industry sectors work under such a regime already. We are very supportive of the principle of alerts being propagated to allies and partners in the right circumstances, which is a very important element of network defence. We do, however, feel strongly that the originator of an alert should be the sole authority in deciding when and how an alert is published. Firstly, there are reputational issues for the victim of an attack, whereas a victim may be perfectly willing to disclose fully to a CERT with confidentiality arrangements in place, that same victim may not wish, and may see no self-advantage, in having any details circulated widely and beyond their control. It may be that victims become reluctant to contact CERTs so as to avoid the risk of reputational damage resulting from the subsequent reporting. This would be a retrograde step, as all victims should be able to report incidents to those who can support and help them without fear of the consequences. Secondly, the three UK government CERTs are part of the national security structure, and have the massive advantage of being able to access sensitive information. This leads to a significant enhancement to our abilities to support customers. We are very concerned that any proposal related to mandatory data sharing would create a tension between our ability to support customers by using sensitive data and the obligations placed upon us to share data within the EU. We are unconvinced that the benefits would come in any way close to balancing the disadvantages. We prefer to see a vibrant voluntary reporting scheme rather than a grudging, minimalist compulsory scheme, and we see the voluntary option as delivering the best benefit to the EU.

© Crown copyright 2012

You may re-use this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence. Visit www.nationalarchives.gov.uk/doc/open-government-licence, write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

This publication is also available on our website at www.bis.gov.uk

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.

URN 12/1222