Department
for Culture
Media & Sport

Reply form for the Public Consultation on Security of Network and Information Systems

Department for Culture Media & Sport

Date: 30 September 2017

Responding to this paper

We welcome your views. To help us analyse the responses please use the online system wherever possible. Visit the Department's online tool (link) to submit your response. Hard copy responses can be sent to:

NIS Directive Team

Department for Digital, Culture, Media & Sport

4th Floor

100 Parliament Street

London

SW1A 2BQ

The closing date for responses is 30 September 2017.

When providing your response, please also provide contact details - we may seek further information or clarification of your views.

This document is also provided in a Welsh language version. Should you require access to the consultation in another format (e.g. Braille, large font or audio) please contact us on 020 7211 6000 or niscallforviews@culture.gov.uk

Copies of responses, in full or in summary, may be published after the consultation closing date on the Department's website.

Freedom of Information

Information provided in the course of this consultation, including personal information, may be published or disclosed in accordance with access to information regimes, primarily the

Department for Culture Media & Sport

Freedom of Information Act 2000 (FOIA) and the Data Protection Act 1998 (DPA).

The Department for Digital, Culture, Media and Sport will process your personal data in accordance with the DPA and, in the majority of circumstances, this will mean that your personal data will not be disclosed to third parties. This consultation follows the UK Government's consultation principles.

If you want the information you provide to be treated confidentially, please be aware that, in accordance with the FOIA, public authorities are required to comply with a statutory code of practice which deals, amongst other things, with obligations of confidence. In view of this, it would be helpful if you could explain to us why you wish that information to be treated confidentially. If we receive a request for disclosure of that information, we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances.

Department for Culture Media & Sport

Association of Financial Markets in Europe (AFME)

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to share our views on the Public Consultation issued by the Department for Digital, Culture, Media & Sport published in August 2017, with a deadline for a response by 30 September 2017.

AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia. AFME is listed on the EU Register of Interest Representatives, registration number 65110063986-76.

Please do not hesitate to contact Emmanuel Le Marois on 44 203 828 2674, email Emmanuel.LeMarois@afme.eu, or David Ostojitsch on 44 203 828 2761, email David.Ostojitsch@afme.eu, should you wish to discuss any of the points.

Department for Culture Media & Sport

AFME's Response:

1. **NIS directive implementation within UK Financial Services**
   The United Kingdom (UK) Department for Digital, Culture, Media & Sport (DCMS) states in its public consultation that "the banking and financial market infrastructure sectors within scope of the Directive will be exempt from aspects of the Directive where provisions at least equivalent to those specified in the Directive will already exist by the time the Directive comes into force. Firms and financial market infrastructure within these sectors must continue to adhere to requirements and standards as set by the Bank of England and/or the Financial Conduct Authority"

   AFME believes that Network and Information Security (NIS) provisions for financial services firms operating in the UK are already in alignment with the requirements of the Network and Information Security Directive and therefore agrees to the position of an exemption for Financial Services.

   While this exemption may apply in the UK due to the level of maturity of financial services in terms if Network and Information Security provisions, encouraged by the Financial Conduct Authority and the Bank of England, this may not be the case in other EU jurisdictions. Indeed, while the directive is a welcome initiative to increase security and resilience across the European Union (EU), the risk of EU jurisdiction developing their own requirements for Financial Services may increase fragmentation across borders, if uncoordinated; and further increase inefficiencies and compliance costs for UK firms operating in different Member States. This may be further exacerbated in the context of on-going Brexit negotiations, with the risk of the UK potentially becoming unaligned to EU directives or legislations.

2. **Financial Sector Competent Authority and Single Point of Contact**
   As stated by the UK Department for Digital, Culture, Media & Sport in its consultation, the UK intends to have multiple sector-based Competent Authorities rather than a single national competent authority. These are not being formally identified for the Financial Sector, who will continue to adhere to requirements and standards as set by the Bank of England and the Financial Conduct Authority (FCA).

   The National Cyber Security Centre is the UK's technical authority on Cyber Security and is proposed as the UK's Single Point of Contact. Single Point of Contacts are expected to act as a liaison on NIS matters in the EU and between National Competent Authorities. Tasks include preparing a summary report of incident notifications and disseminating cross border incidents to other Member States.

   AFME believes further clarity would be welcome to understand the roles and responsibilities of the Financial Sector Competent Authorities and it's Single Point of Contact in the event of a major cyber threat. For instance, will the

Bank of England and the Financial Conduct Authority exchange information with the NCSC (e.g. the UK CSIRT), in the same manner as other Competent Authorities from other sectors? How will useful information regarding a potential threat be used, aggregated and shared by these actors, to support cyber resilience of critical infrastructures, within the UK and across Member States?

Furthermore, additional clarity could be provided to firms operating in multiple Member States and therefore potentially falling in scope of the NIS directive across multiple jurisdictions. Would such firms have to report incidents to each regulator in such a case?

3. **Security requirements for Operators of Essential Services**

As indicated in its consultation Operators of Essential Services (OES) will need to "take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems in the provision of their service" and "take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used in the provision of their service".

AFME welcomes the UK DCMS view on a "principles based approach" for the Network and Information Security directive implementation in the UK. Indeed, AFME believes that only a principle based approach may allow firms to effectively prepare for cyber threats. As articulated in the Financial Stability Institute of the Bank for International Settlements Insights Paper, "Regulatory approaches to enhance banks' cyber-security frameworks", published in August 2017: "the risk exists that regulation becomes too prescriptive, so that it falls behind both the constantly evolving threat from cyber-risk and advances in cyber-risk management" (p.4).

AFME understands that the intention is for the National Cyber Security Centre (NCSC) to develop i) high level security principles all operators are expected to comply with and ii) a generic cross sector security including a Cyber Assessment Framework (CAF). While AFME is supportive of a principle based approach, these principles should be developed in alignment with existing international standards to allow for a common approach across sectors and across Member States. This is particularly important for firms operating across multiple jurisdictions which may therefore fall under the scope of an OES in more than one Member State.

AFME believes further clarity on how the risk of diverging principles and guidance may be reduced between sectors and Member States. This would support efforts by critical infrastructures operating in multiple jurisdictions, tackling cyber-attacks from a global perspective. In particular for Financial Services firms, AFME is looking forward to the publication of principles and

the CAF by the NCSC, and how these will be adopted by the Bank of England and the FCA, to ensure harmonisation across sectors.

4. **Incident reporting**

AFME acknowledges the change in incident report requirement under the NIS directive implementation. Indeed, incident report requirements are intended to be reinforced for certain types of incident, ensuring that competent authorities and the NCSC are aware of significant disruptions to the services provided by the sectors in scope:
All NIS incident reporting will be to the NCSC as the dedicated Computer Security Incident Response Team (CSIRT) for the UK;
A reportable incident is one that has a significant impact on the continuity of essential services;
Voluntary reporting is encouraged to cover potential disruption of services
The timeframe for reporting is defined as "without undue delay and as soon as possible, at a maximum no later than 72 hours after having become aware of an incident".

AFME views that further transparency and clarity, on how cyber incident reporting requirements may support global cyber resilience, would benefit Financial Services and other sectors in the event of a cyber-attack. AFME encourages the on-going dialogue in this area, such as between Authorities, the NCSC and sector; as well as the development of tools that may support coordination efforts (e.g. development of a UK guide on who to call in the event of a cyber-attack). Clarity on how this cooperation could work across Member States would be beneficial for firms operating in multiple jurisdictions tackling with a potentially global threat.

Furthermore, for firms operating in multiple Member States and therefore potentially falling in scope of the NIS directive across multiple jurisdictions, further clarity could be provided for incident reporting. Would such firms have to report incidents to each regulator in such a case, increasing the burden of having to report incidents to different regulators and supervisors simultaneously?

5. **Penalty Regime**

AFME acknowledges the proposed two bands of penalty regimes presented by the DCMS, intentionally similar to the that of the general Data Protection Regulation (GDPR). As indicated by the DCMS, AFME views that financial penalties should only be levelled as a last resort where it is assessed appropriate risk mitigation measures were not in place without good reason. In addition, the aforementioned penalties should be considered as maximum penalties, used in the most egregious incidents. It is expected that mitigating factors including sector-specific factors will be taken into account by the Competent Authority when deciding appropriate regulatory response.

AFME is concerned with the risk of Penalty Regimes becoming disproportionate. If penalty regimes of such magnitude (e.g. 4% of annual turnover) become common practice and are embedded in multiple regulations or directives, such as the NIS directive and the GDPR, this may have a multiplying effect in the case of an incident. This could lead to disproportionate penalty regimes which may penalise firms over and above what is appropriate, potentially jeopardising their operations.