Technology and Operations – Cybersecurity Working Group

AFME Position Paper on the EU Cyber Security Act and Package

The following document is a proposed AFME position paper for the Cybersecurity Working Group. The position paper includes the following sections: (1) Executive Summary, (2) ENISA Mandate Revision; (3) EU-wide Voluntary Cyber Security Certification Scheme; (4) EU Cybersecurity Blueprint; (5) Cybersecurity Emergency Response Fund; (6) European Cybersecurity Research and Competence Centre & Digital skills and jobs coalition; (7) International cooperation; (8) Conclusions; (9) Working Group Overview and Contacts

1. Executive Summary:

AFME welcomes the increased focus of the European Commission on the importance of cybersecurity in the EU. Overall, the proposed cybersecurity legislative package[1] and the suggestions communicated by European Commission on "Resilience, Deterrence and Defence: Building a strong cybersecurity for the EU"[2], are considerable improvements to the 2013 Cybersecurity Strategy, and an important step towards the safe, secure and resilient adoption of a EU Single Market.

Financial Services are often cited as a prime target for cyber-attacks because of their pivotal role in the economy, as providers of critical services. Because of their systemic importance, financial service firms have invested in large scale cyber security programs. However, with an increasingly complex, interconnected and fast evolving landscape, cyber policies need to keep in mind the global picture and remain pragmatic, so that firms can dedicate scarce resources where it matters and respond to time critical attacks as a coordinated network.

AFME believes cybersecurity is a global issue, which requires a pluri-disciplinary and multi-stakeholder approach, of both private and public sectors, to maintain the security and stability of our economy.

AFME has provided comments against the key points included in the package:

- ENISA Mandate Revision
- EU Voluntary Cyber Security Certification Scheme
- EU Cybersecurity Blueprint
- Cybersecurity Emergency Response Fund
- European Cybersecurity Research and Competence Centre & Digital skills and jobs coalition
- International cooperation

2. ENISA Mandate Revision (part of the cybersecurity legislative package)

The first element of the cybersecurity legislative package is a revision of the current mandate of the European Union Agency for Network and Information Security (ENISA), setup in 2004, laying down a renewed set of tasks and functions:

- ENISA to be granted a permanent mandate.
- ENISA's to act as a reference point in the EU ecosystem and working in close cooperation with other relevant EU bodies
- ENISA's organisation and governance to be moderately reviewed to reflect the needs of the wider stakeholder's community
- ENISA's scope and mandate reinforced and delineated around key activities such as the NIS Directive, the EU Cybersecurity Strategy, the EU Cybersecurity Blueprint and the voluntary certification for ICT security, in particular:

[1] https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505316068800&uri=JOIN:2017:450:FIN

- **EU policy development and implementation**: ENISA to act as EU advisor, overseeing NIS directive implementation consistency cross-border and sector, provide reports on the EU legal framework.
- **Capacity building**: ENISA tasked with the improvement of incident reporting & cyber security supervision, supporting the establishment of sector Information Sharing and Analysis Centres (ISAC's).
- **Knowledge and information, awareness raising:** ENISA to become the information hub of the EU.
- **Market related tasks**: ENISA to analyse the cybersecurity market to identify ways to better match demand and supply, supporting the EU policy development in ICT cybersecurity certifications.
- **Research and innovation**: ENISA to advise EU and MS on priorities for research & development.
- **Operational cooperation and crisis management**: ENISA to upgrade cyber security exercises ("Cyber Europe"), to take role of secretariat of CSIRT's Network, potential assistance to MS.
- **EU cybersecurity blueprint role**: ENISA to facilitate cooperation between Member States.

Overall AFME welcomes the revised scope and mandate of ENISA, in particular the agency will be provided with a permanent status and additional resources. AFME would like to add the following comments:

- **Status of ENISA, resources and geographical location:** AFME believes that for ENISA to act as a reference point in the EU ecosystem, working in close cooperation with other relevant EU bodies, the agency should be provided with the appropriate level of resources and geographical locations, allowing coverage of its geographical remit and frequent engagement with its stakeholders. For instance, ENISA could have dedicated "relationship manager" for each Member State. Such "relationship manager" could support both public and private sectors' representatives belonging to the specific Member State thus expanding its geographical footprint. AFME believes that with the current planned increase it may be difficult for ENISA to fulfil this ambitious role.
- **Organisation and Governance**: AFME believes the agency's structure should reflect its broadened scope and footprint to ensure it is successful in achieving its goals. It is not clear what are roles & responsibilities attributed to EU supervisory authorities in relation to cyber security such as the ECB, the EBA, versus ENISA, and the interplay with Member State NCA's. AFME believes further clarity in this area, taking the shape of practical scenarios would be particularly helpful, to ensure effective policy development and implementation, to avoid potential conflicting or duplicative requirements, which would reduce overall sector resilience and coordination in the event of large scale attacks.
- **EU policy development and implementation:** There is currently a risk of EU jurisdictions developing prescriptive or un-aligned requirements for Financial Services and other sectors in the NIS directive implementing. AFME believes it will be key for ENISA to achieve a harmonised implementation of the NIS directive across Member States to create a common and consistent baseline for cyber resilience in Europe.
- **Capacity building:** AFME believes the improvement of incident reporting and information sharing via ISAC's will be key to the success of increased preparation and response of private and public sector. A common taxonomy on incident reporting would be beneficial to clarify and harmonise regulatory expectations (such as a common terminology, thresholds, timelines…) and help firms report relevant incidents. In addition, financial services would benefit from aggregated cross-border and cross-sector information, if timely, to prepare and respond more effectively to incidents effecting other regions or sectors or that may be detected only once aggregated.
- **Knowledge and information, awareness raising:** AFME welcomes the initiative to have a central hub for information sharing and distribution at EU level. While in principle useful, ENISA would have to consider how to add value to what is currently used, recognised and trusted by market participants and how this would fit in the global context. Organisations such as the FS-ISAC already provide valuable information sharing, and other related services, to Financial Services firms who operate globally and therefor any additional information sharing service if not relevant may not provide the extent of benefits expected.
- **Market related tasks (standardisation, cybersecurity certification):** AFME welcomes the future role of ENISA as a market observatory for the uptake of cybersecurity standards across the EU. There are many

currently existing and recognised standards used by firms, national and international, and there would be significant benefit in ensuring these are recognised and applicable across Member States. However, AFME would caution the establishment of a new standards and certifications which would increase firm's costs and complexity of compliance, even if voluntary, and further accentuate fragmentation. An effort should be made so as to acknowledge existing certifications and make them compatible so as to avoid the burden to comply with the same security controls in different certifications already applied.

- **Research and innovation:** AFME welcomes the future role of ENISA on contributing to the Public-Private partnership on cybersecurity in areas such as the European Cybersecurity Research and Competence Centre (ECRCC) and providing guidance on R&D efforts in the EU. Public-private partnerships can be an effective forum to raise awareness and education between public and private sector and identify areas of cross-sector benefit. Furthermore, AFME views this as a potential avenue to address the cyber security skills gap, currently projected to reach 1.8 million jobs worldwide by 2022[3].
  AFME believes cyber security requires cooperation of public and private sector, as articulated in the 2011 UK Cyber Security Strategy and the NIS Public-Private Platform launched in 2013[4] on achieving the goal of a safe, secure internet: "achieving this vision will require everybody, the private sector, individuals and government to work together. Just as we all benefit from the use of cyberspace, so we all have a responsibility to help protect it."
- **Operational cooperation and crisis management:** AFME welcomes the future stream of work building on strengthening operational and EU capabilities crisis management. On the one hand, on crisis management, AFME believes further clarity should be considered on how across sectors the CSIRT network will operate in conjunction with other key EU institutions, such as the EBA, the ECB, Europol, EC3 and ENISA, and the roles and responsibilities of each of these actors. The creation of playbooks which can focus on different scenarios may provide a very concrete view of the communication (e.g. incident reporting, information sharing) and actions required of the various actors to ensure resilience is effective in context. AFME believes cyber exercises are an important step to ensure these playbooks are understood by all actors and must remain relevant to the real threats faced by actors locally and in aggregate. Consequently, given the cross-border nature of cyber security AFME views significant benefit in conducting cyber exercises that can bring together other jurisdictions (e.g. US, APAC). Technologies such as sand-boxes could be an effective and safe tool for conducting these tests and exercises, where inclusion of appropriate data protection instruments could be identified and included. On the other hand, on operational support, while AFME is encouraged by the potential role of ENISA in assisting Member States on training and handling incidents, the currently planned increase of resources and funding of ENISA may not be sufficient to address demand. However, this may be more rapidly and effectively addressed by becoming a key partner in fostering collaboration amongst Member States, between public-private sector and across sectors, while establishing itself as a key international partner.
- **Role of ENISA in the EU cybersecurity blueprint:** As indicated in AFME's comment on "Operational cooperation and crisis management" a EU cybersecurity blueprint (see section "4. EU cybersecurity blueprint" below) could have great value in increasing EU cyber resilience by ensuring there is a clear understanding of the expected actions, roles and responsibilities of all actors involved (Private sector, CSIRT's, ISAC's, EU Institutions such as ENISA and the ESA's) in different types of cyber related events (e.g. scenarios of a playbook). However, AFME believes completing such a blueprint could be challenging as for the EU cybersecurity blueprint to be relevant for market actors in the case of a real threat, it will have to be readily available by all, relevant to potentially real and unknown global threats, and implemented to be time critical, as threat responses are often a matter of minutes if not seconds. AMFE would welcome the opportunity to use industry lessons learned to help shape the EU cybersecurity blueprint from the perspective of Financial Service sector.

To conclude, AFME views that one centrally empowered body with sufficient resources and governance powers is beneficial to the financial system, however clear demarcation is required as to the role and interaction within the existing framework. AFME believes further clarification is required regarding:

[3] https://iamcybersafe.org/research_millennials/
[4] https://ec.europa.eu/digital-single-market/en/news/nis-public-private-platform-%E2%80%93-call-expression-interest

- How ENISA will coordinate with other ESA's (ECB, EBA, ESMA) and with Member States regulators and supervisors;
- Expectations around conferring regulatory authority to ENISA;
- The legal framework within which ENISA will operate;
- How Financial Services sector will be involved in shaping ENISA; and
- The details as to how ENISA is able to share information.

3. EU-wide Voluntary Cyber Security Certification Scheme (part of the cybersecurity legislative package)

The second element of the cybersecurity legislative package is the establishment of a European Cybersecurity Certification Framework (the "Framework") for ICT products and services, allowing certificates issued under the framework to be valid and recognised across all Member States. The objective of the certification is to address current market fragmentation and benefit citizens, business by driving more jobs and growth and reducing barriers in the internal market. Key elements of the framework:

- Definition of security objectives to design a European cybersecurity certification scheme: minimum requirements, products categories, evaluation criteria and method;
- Certifications are to be prepared by ENISA with the assistance of the European Cybersecurity Certification Group e.g. ECCG (composed of member state national certification supervisory authorities) and adopted by the Commission by means of implementing acts;
- The certifications are to remain voluntary unless otherwise provided in Union legislation;
- Accreditations are to be issued by a conformity assessment body and are issued for 5 years;
- Member States designated authorities are to monitor, supervise and enforce certifications;

While AFME views significant benefit in addressing market fragmentation and seeking to establish consistent best in class practices across jurisdictions, even outside of the EU, the creation of voluntary EU cyber certification may not be the only or best way to achieve this goal. Indeed, while certifications can be a useful tool to promote standards and drive more trust, the activity of creating, issuing, monitoring (e.g. auditing) and maintaining a certification can be complex and burdensome, in particular for ICT products, which require a principle and risk-based approach due to the complex and evolving nature of cyber threats.

In addition, while the certifications coming out of the framework may help reduce barriers within the EU single market, it may erect additional barriers with regards to other jurisdictions, which could be burdensome for firms operating globally. In this case this will lead to additional complexities, increasing operational and compliance costs for those firms, even if voluntary.

Furthermore, it is AFME views that there are currently established, globally and regional industry recognised certifications in ICT products and services. Therefore, any new certificate would have to provide real business value incrementally to what the market currently uses. As such, there may be more benefit in achieving mutual recognition of those already in use certificates rather than creating new ones. An effort should be made so as to acknowledge existing certifications and make them compatible so as to avoid the burden to comply with the same security controls in different certifications already applied.

Regarding the different steps of the framework, AFME believes private sector ought to be more involved in the definition of securities objectives, as potential end users of the certifications, and assisting ENISA and the ECCG in the preparation phase. Indeed, Financial Service firms are widely regarded as a mature industry with regards to cyber security and their input would be beneficial in these steps of the framework's process. This is valid for other industries as well. The proposal should be more explicit about the openness and transparency during the preparation and adoption of the certification schemes, to allow industry and standard setting bodies to be more directly involved. Doing so would provide diverse expertise and knowledge necessary to ensure the correct design of the certification schemes.

AFME emphasizes on maintaining the voluntary nature of the EU cybersecurity certification framework and further clarity should be provided to firms if this could be provided in Union legislation.

Finally, a clearer definition should be provided to the term "ICT products and services" so firms can have a better understanding of how this scope applies to the certification framework.

To conclude, AFME believes the proposal for a EU-wide Voluntary Cyber Security Certification Scheme requires a more appropriate governance system and additional details for completeness. Such as practical implementation matters (e.g. compulsory versus voluntary), how this would fit with international regulations and generally how this would part of the blueprint of coordination (e.g. with details of information flows in possible circumstances) and cyber fund.

4. EU cybersecurity blueprint (Non-legislative)

Please see comments provided in section "3. ENISA Mandate Revision". The blueprint should aim to cover the entire life cycle of the crisis management even if there will be challenges to design and implement.

5. Cybersecurity Emergency Response Fund (Non-legislative)

AFME understands that in the joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", published September 13th[5], that a Cybersecurity Emergency Response Fund would allow Member States to benefit from help under a major incident, provided the appropriate due diligence had been implemented prior to the incident. AFME believes further clarification should be provided with regards to the practical implications on the due diligence requirements and as well how the response fund could benefit public and private sector.

6. European Cybersecurity Research and Competence Centre & Digital skills and jobs coalition e.g. ECRCC (Non-legislative)

AFME understands that in the joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", published September 13th, that the EU would benefit from building on public private partnerships, connecting Member States networks of cybersecurity competence centres with the ECRCC at its centre. This structure would help coordinate research and competences, stimulate developments of technology in cybersecurity (such as artificial intelligence, quantum computing, blockchain and secure digital identities), complement capacity building in efforts, pooling and shaping research efforts. Furthermore, this would support industry through testing and simulation.

AFME welcomes overall such an initiative, which aims to build on existing capabilities existing at Member States level, however, further clarifications would be required to understand how the ECRCC would avoid duplications. In addition, AFME believes further details regarding the implementation aspects or how the ECRCC would work, would help clarify the exact expected role of the ECRCC, such as its potential role as a capability project manager (e.g. what capabilities?) or to provide access to mass data for EU companies (e.g. how will it be obtained, managed and maintained?).

7. International cooperation (Non-legislative)

AFME welcomes that in the joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", published September 13th, the Commission has put forward a proposal on the European Agenda on Security, to facilitate cross-border access to electronic evidence, the implementation of practical measures to improve cross-border access to electronic evidence for criminal investigations, and the standardisation of judicial cooperation forms used between Member States.

AFME believes that these measures will positively increase efficiency in the "Response" phase but efficiencies should be considered in all phases of a cyber threat (Prevention, Preparedness, Response, and Recovery). Furthermore, while the Cybersecurity package will provide efficiencies in other parts of the phases, AFME believes, cyber threats may only be effectively tackled via the adoption of an international law applied to the cyberspace, permitting law enforcement and

[5] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450

other stakeholders to prosecute against any type of cyber-attack. This idea is advocated by Microsoft and has been discussed at the world economic forum[6]. AFME would urge the EC to bring this point forward at the next G7 meeting, to reach an agreement on common measures and next steps.

8. Working Group Overview and Contacts

Firm	Attendee	Contact
BAML	Nicholas Tuppen	nicholas.tuppen@baml.com
Barclays	Aatif Ahmad	aatif.ahmad@barclays.com
Barclays	Paul Shaw	paul.shaw@barclayscapital.com
Barclays	Lewis Honour	lewis.honour2@barclayscorp.com
BBVA	Borja Larrumbide Martinez	fborja.larrumbide@bbva.com
BNP Paribas	Frederic Hustache	frederic.hustache@uk.bnpparibas.com
BNP Paribas	Johan Noleau	johan.noleau@uk.bnpparibas.com
BNY Mellon	James Thomas	james.thomas@bnymellon.com
BNY Mellon	Scott MacDougall	scott.macdougall@bnymellon.com
BNY Mellon	George Stephens	george.stephens@bnymellon.com
BNY Mellon	Anna Solar Bassett	Anna.Solar-Bassett@bnymellon.com
Citi	Anthony Hines	anthony.hines@citi.com
Citi	Gulrez Jamadar	gulrez.jamadar@citi.com
Citi	Cal Waits	cal.waits@citi.com
Citi	Patrick Moran	patrick.moran@citi.com
Citi	Charlotte Branfield	charlotte.thoms.branfield@citi.com
Credit Suisse	Adriana Ennab	adriana.ennab@credit-suisse.com
Credit Suisse	Chris Girling	chris.girling@credit-suisse.com
Deutsche Bank	Norbert Schiffner	norbert.schiffner@db.com
Deutsche Bank	Nadim Shehadeh	nadim.z.shehadeh@db.com
Goldman Sachs	Richard Benett	richard.bennett@gs.com
HSBC	Carlton Cristie	carlton.cristie@hsbc.com
HSBC	Elena Pullin	elena.pullin@hsbc.com
HSBC	Sarasi Randombage	sarasi.randombage@hsbc.com
HSBC	Timoty Clausen	timothy.j.clausen@hsbc.com
Intesa San Paolo	Cusma Lorenzo Giorgio	giorgio.cusmalorenzo@intesasanpaolo.com
Intesa San Paolo	Lonati Corrado	corrado.lonati@intesasanpaolo.com
Intesa San Paolo	Maria Adele Di Comite	mdicomite@nikegroup.it
Intesa San Paolo	Raffaella Donnini	raffaella.donnini@intesasanpaolo.com
Intesa San Paolo	Marco Boscolo	marco.boscolo@intesasanpaolo.com
JP Morgan	Hem Pant	hem.pant@jpmchase.com
JP Morgan	Renata Gal	renata.gal@jpmorgan.com
JP Morgan	Stephen Colletti	stephen.j.colletti@jpmorgan.com
JP Morgan	Sam Jones	samuel.jones@jpmchase.com
Lloyds	Giles Taylor	giles.taylor@lloydsbanking.com
Lloyds	Ben Payne	ben.payne@lloydsbanking.com
Morgan Stanley	Peter Troy	peter.troy@morganstanley.com
Natwestmarkets	Juan Rodriguez	juan.rodriguez@natwestmarkets.com
Nomura	Andy Bartram	andy.bartram@nomura.com
Societe Generale	Frank Ebrard	franck.ebrard@sgcib.com

[6] https://www.weforum.org/agenda/2017/12/why-we-urgently-need-a-digital-geneva-convention

Standard Chartered	Julia McKenny	JuliaNicole.McKenny@sc.com
UBS	Dave Evans	dave.evans@ubs.com
UBS	Carlo Hopstaken	carlo.hopstaken@ubs.com
UniCredit	Pierluigi Carbone	pierluigi.carbone@unicredit.eu
UniCredit	Filippo Burrone	filippo.burrone@unicredit.eu
UniCredit	Andrea Serati	andrea.serati@unicredit.eu
UniCredit	Matteo Lancelotti	matteo.lancellotti@unicredit.eu

Association of Financial Markets in Europe (AFME)

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to share our views on the Consultation Paper issued by the European Banking Authority (EBA)
published on 18 May 2017, with a deadline for a response by 18 August 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.

Should you wish to discuss any of the points 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.