EU Cyber Security Certification (EU Exit) Call for Views

BEAMA Response

About BEAMA

BEAMA is the UK trade association for manufacturers and providers of energy infrastructure and systems. We represent more than 200 companies, from start-ups and SMEs to large multinationals. Our members provide HVAC products, EV infrastructure, electrical transition and distribution equipment, energy storage and flexibility assets in networks and the built environment, to support a safe and secure low carbon energy system.

BEAMA has been very active since the referendum result to ensure industry can be closely aligned with the work of UK Government to establish the most suitable trade system and regulatory framework for our sector post Brexit. We established EURIS[1] following the referendum result and from the outset EURIS has supported the principle of regulatory alignment, especially for products, post Brexit.

BEAMA response

There is a clear business need for the continued dynamic alignment of UK and EU product regulation and certification requirements. As the UK leaves the European Union, the challenges and risks posed by regulatory divergence are of primary concern to BEAMA members. Regulatory divergence is a serious threat to industry and will add significant cost to many UK products; evidence from BEAMA members suggests that in some cases it will encourage the movement of business out of the UK. BEAMA therefore calls on Government to work with us and our members to ensure appropriate dynamic regulatory alignment after the UK leaves the EU.

The need for regulatory alignment is especially pertinent to cyber security. Diverging on security requirements and software in products sold across the EU and in the UK could add cost and complexity to accreditation and assurance schemes and create opportunities for threats and cyber-attacks. BEAMA has consistently advocated a system of internationally aligned cyber security requirements and cautions Government not to prescribe a UK-specific method by which agreed cyber security outcomes are achieved or compliance demonstrated.

BEAMA contributed to the drafting of the EU Cybersecurity Act. We accept this new Act and the mandate on ENISA to develop aligned EU product certification schemes. BEAMA will retain its membership of EU trade associations[2] after the UK has left the EU and will continue to engage with the process of developing and drafting new EU legislation, regulation and standards.

Along with DCMS, BEAMA recognises the critical need to ensure the cyber security of consumer products and services and to promote consumer confidence in such products and services. We have

[1] http://www.euristaskforce.org/about-euris/ - European Union Relationship and Industrial Strategy Task Force – an advisory body for the potential impacts of the changing relationship between the UK and EU for the UK Government, manufacturers and the media. EURIS has 13 trade association members representing £153billion in UK turnover.

[2] APPliA, Orgalim, T&D Europe, CECAPI, EUHPA, EVIA, AquaEUropa

been active in the UK and Europe in developing and promoting cyber security best practice. As stated in previous consultation responses, BEAMA and its membership recognise the importance of promoting and maintaining common standards and certification processes across Europe to reduce costs for consumers and increase the cyber security of products. BEAMA members oppose measures that would lead to the UK diverging from European common approaches. We invite the Government to work with us in support of efforts to align UK, European and international approaches to cyber security.

Regarding the four principles set out on the consultation paper, BEAMA's response is:

1. Hypothetically, there may be two reasons for the UK to conclude that an EU cyber security certification was not in the interests of improved cyber security:
    a. Because it was unnecessary, in which case there would be no need to introduce it in the UK but UK manufacturers would likely have to comply with it for any sales in Europe; or
    b. Because the scheme was considered defective, in which case the UK should be mindful of avoiding an insistence on 'perfection'. A European scheme that could be improved but has no fundamental weakness will be preferable to a UK-only scheme that avoids a minor defect but then isolates the UK market.
2. It is not clear that UK customers will always be aware of the need for certified products, so they may need a proxy to represent them.
3. Agreed, but there may be tension between different businesses areas, for instance between those that manufacture products and those that use them.
4. A high bar should be set for this barrier. We must not diverge from European approaches on the basis of minor disagreement.

BEAMA would like to add a fifth principle to the list when Government is determining the approach to each EU scheme:

5. If the EU scheme is not aligned with in the UK: that there is no risk to the business and industry

This fifth principle would require an assessment of the risk of regulatory divergence. While we agree with the four principles already set out, Government and Industry need to consider the risk to UK sectors of not aligning with the EU. This could be challenging to equate, but it is something that must be factored into risk assessments as we review alignment with EU regulations after the UK leaves the EU. BEAMA is also investigating how to include this principle in risks assessments of other product regulations, including Ecodesign and energy labelling, whereby with the introduction of a new regulatory measure under these regulatory frameworks in the EU, the UK would seek to consult industry on alignment in equivalent UK regulations. Any principles followed in delivering this alignment must factor in benefits and costs appropriately.

In the call for views, DCMS mentions other assurance schemes involving certification that have been applied to the GB smart metering infrastructure. These include Common Criteria, based on an international cyber security standard and CPA (Commercial Product Assurance). While this is aligned with ISO standards, the smart metering cyber security requirements are specific to GB and not harmonised across Europe. This can be justified for a rollout of infrastructure not purchased by the consumer and as part of a government-led mandate, but it is an example of how a GB-specific certification and assurance process increases the cost and time taken to deploy infrastructure. BEAMA's view is that this is not a repeatable process for the wider IoT product market, and imposing

such a GB- or UK-specific scheme on other digital IoT products would be a significant constraint on the market. A better approach is to ensure that the provisions and requirements of the EU Cybersecurity Act are adopted in the UK to deliver a harmonised solution that will foster innovation and competition and deliver the highest standards of cyber security at reasonable cost.

We welcome continued discussion with DCMS on this topic. Please contact John Parsons, Director of Digital at BEAMA john.parsons@beama.org.uk