EU Cyber Security Certification (EU Exit) Call for Views

Call for views on the UK's proposed approach to cyber security certification as currently regulated by *Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)* following the UK's departure from the EU.

Background

The EU Cyber Security Act entered into force on 27th June 2019. The Cyber Security Act provides the EU Cyber Security Agency (ENISA) with a strengthened and permanent mandate and establishes a cyber security certification framework under which EU-wide cyber security certification schemes will be developed and implemented.

The UK has previously operated a number of assurance schemes involving certification, including Common Criteria, based on the international cyber security standards (ISO standards 15408/18045), and CPA (Commercial Product Assurance), based on National Cyber Security Centre (NCSC) or Industry developed security characteristics. The UK participates in two mutual recognition arrangements which are based on Common Criteria, including CCRA and SOG-IS MRA.

The EU Cyber Security Act looks to harmonise those certification schemes operated within the Union in order to strengthen the digital single market and increase trust for consumers of ICT products and services.

The UK was actively engaged in the development of the Cyber Security Act, and remains committed to enabling improved cyber security across Europe and preventing unnecessary market fragmentation.

Summary

The Regulation sets out that the Digital Single Market, and in particular the data economy and IoT, can thrive only if there is general public trust that such products, services and processes provide a certain level of cyber security. It does not introduce directly operational certification schemes, but creates a system which allows voluntary cyber security certification schemes to be established and recognised across the EU. These certification schemes would attest that the ICT products, services and processes that have been evaluated comply with specified security requirements. Connected and automated cars, electronic medical devices, industrial automation control systems and smart grids are provided as some examples of sectors in which certification is already widely used or is likely to be used in the near future.

The European Commission will publish a Union wide rolling work programme which will identify strategic priorities for future European cybersecurity certification schemes, including a list of ICT products, services and processes that might be included in the scope of a scheme. On the basis of this, the Commission they may request ENISA (the EU Cyber Security Agency) to prepare a scheme. In some cases, the Commission or the Member

States, via the European Cyber Security Certification Group, may request a scheme directly to ENISA.

The framework requires that each certification scheme:

i. is designed to achieve a number of security objectives as set out in the Act.
ii. may specify one or more assurance levels (basic, substantial, high).
iii. may allow for conformity self-assessment.
iv. includes a number of other elements such as: scope, references to standards, evaluation criteria, conditions for marks or labels, rules concerning vulnerability disclosure, validity period, conditions for mutual recognition with third countries.
v. provides supplementary cybersecurity information as set out in the Act.

Proposed approach

The UK is committed to maintaining a close relationship with the EU on cyber security following our departure from the EU, and will seek to cooperate on approaches to cyber security certification with the EU.

The EU recognises in the Cyber Security Act that supply chains are global and that the introduction of certification schemes should seek to reduce market fragmentation. The Regulation therefore makes provision for mutual recognition arrangements on specific schemes to be agreed with third countries, with cyber security certification schemes implemented under the framework specifying conditions for such agreements.

It is the UK's understanding that such arrangements would mean that there is provision within the Act for the UK and the EU to mutually recognise one another's cyber security certification schemes, meaning that UK issued certificates would serve the same purpose in EU markets as EU issued certificates and vice versa.

The UK will therefore seek to enter into negotiations with the EU on mutual recognition arrangements under the terms set out by those schemes, where it seems reasonable to do so and subject to agreement with the EU.

In preparation for transmitting an EU Cybersecurity Certification Scheme to the European Commission for adoption, ENISA is required to consult all relevant stakeholders and take into account the opinion of Member States, through their membership of the European Cybersecurity Certification Group. In the same way, the UK would look to work with experts and industry on the potential for entering into such arrangements for future certification schemes, as and when they are proposed, through its own stakeholder consultation groups which will consider each scheme on a sector by sector basis. DCMS will take the lead alongside the relevant Lead Government Department in any consultation on industry or consumer demand for a scheme.

It is proposed that the UK would look to ensure that the following principles are applied when determining its approach to each EU scheme proposal:

1) The EU scheme proposal would contribute to better cyber security in the UK

The proposal to introduce any EU cyber security certification must be assessed by the relevant UK Government authority and the NCSC to be in the interests of improved cyber security.

2) The EU scheme proposal meets a consumer need

   There is a clear demand from UK consumers of the certified product, service or process for the UK to engage in the scheme.

3) The EU scheme proposal provides economic advantage to UK business

   The UK will hold the interests of UK business paramount. We will work to ensure that a cost benefit analysis shows an evidence based economic benefit to UK business.

4) The EU scheme proposal must be open and transparent

   The UK believes that open and transparent approaches are an essential way of improving global cyber security. The UK will only engage where we believe this to be the case.

It is the understanding of the UK Government that even if the UK does not engage or develop a mutual recognition approach for a specific EU scheme this will not necessarily preclude UK companies from gaining EU certification for their products or services via an EU member state. This will depend on the conditions set out within each individual scheme.

Call for views

The Government is seeking views on this proposed approach. We would welcome views and any supporting evidence on this proposal.

How to respond

Email responses can be sent to: eucybersecurityreg@culture.gov.uk

Postal responses can be sent to:

EU Cyber Security Team (4/48)
Department for Digital, Culture, Media and Sport
100 Parliament Street
London
SW1A 2BQ

The closing date for responses is Tuesday 15th October 2019.

When providing your response, please also provide contact details as we may seek further information or clarification of your views. A summary of responses may be published after the consultation closing date on the Department’s website.

Further information

Information provided in response to this call for views, including personal information, may be published or disclosed in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000 (FOIA), the General Data Protection Regulations (GDPR), and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and 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 regard the information you have provided as confidential.

If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding.

We’ll process your personal data in accordance with the Data Protection Act 2018.