Department for Digital, Culture, Media & Sport

Margot James MP
Minister for Digital and the Creative Industries
4th Floor
100 Parliament Street
London SW1A 2BQ

www.gov.uk/dcms
enquiries@culture.gov.uk

Sir William Cash MP
Chair of the European Scrutiny Committee
House of Commons
London
SW1A 0AA

TO2018/07325/DC
15 May 2018

Dear Bill,

I am writing in response to the Committee's communication dated 21st February regarding 12183/17 (under scrutiny 12208/17): the Regulation on ENISA and Cyber Security Certification. I am pleased to be able to respond to the additional issues raised by the Committee and to provide a general update on the negotiations.

Comitology Procedure

In your communication you note that the advisory comitology procedure is proposed for the European Cybersecurity Certification Group and you seek clarification as to whether the Government intends to press for the more stringent examination procedure to be used instead, and, if not, to provide its reasons.

Article 44 of the proposed Regulation sets out the provisions for the preparation and adoption of a European cybersecurity certification scheme. Following a request for a scheme by the Commission or the European Cybersecurity Certification Group (the "Group"), ENISA is responsible for the preparation of such a scheme. The Group is required to provide its expert advice and opinions in the preparation of a scheme and before it is submitted to the Commission. While the Group is not subject to a formal voting procedure within in the Act, developments within the text have provided reassurance that ENISA will take account of the opinion of the Group before transmitting it to the Commission.

The Commission, based on the scheme proposed by ENISA, may then adopt implementing acts in accordance with Article 55(2). Article 52(5) provides that those implementing acts must be adopted in accordance with the examination procedure. Article 55(2) makes clear that Article 5(4)(b) of Regulation (EU) No 182/2011 applies. This means that, any draft implementing act cannot be adopted if there is no opinion delivered by the committee. The more stringent examination procedure is therefore used here.

Further information regarding future UK-EU co-operation in the area of cybersecurity

The cyber threat the UK and its European allies face from state actors and cyber criminals remains significant and knows no international boundaries. The UK and EU Member States share a single cyberspace and so, as each country improves its defences, we all become collectively stronger.

To contend with a truly global threat such as this we need a truly global response - with not only the UK and EU, but industry, government, like-minded states and NATO all working together to strengthen our cyber security capabilities. The UK is one of the world's leading digital nations and a leader in the field of cyber security. We have accordingly taken a central role, both as an EU Member State and internationally, to push forward the cyber agenda.

The UK is ready to maintain and deepen our shared ability to support our collective security, and to uphold our values and protect our democratic processes, by responding robustly to state based threats and cyber criminals.

Implications of non-participation in ENISA and the CSIRT network

Membership of the European Network and Information Security Agency (ENISA) is one of the ways in which the UK discusses cyber security policy and shares expertise with European partners.

The CSIRT Network is a network of cyber response teams across Europe and its purpose is to promote swift and effective operational cooperation in the event of a cyber security incident. Information sharing is voluntary and the Government has found the CSIRT Network to be a useful forum in which the UK can share cyber threat information to help protect the UK and our European partners from common threats to our economy, democratic processes and Critical National Infrastructure (CNI). The National Cyber Security Centre represents the UK in the CSIRT Network.

If the UK does not secure agreement to participate in the ENISA Management Board or the CSIRT Network we would instead use our bilateral relationships with EU Member States to share expertise and information.

The UK will continue to work together with the EU to promote strategic frameworks for conflict prevention, cooperation and stability in cyberspace. These frameworks should consist of: the application of existing international law; the implementation of voluntary, non-binding norms of responsible state behaviour; and the development and implementation of practical cyber confidence building measures between states.

General update on the Negotiations

In our Explanatory Memorandum of 18th October and subsequent letter of 19th January, we outlined the envisaged role for ENISA, including the proposed tasks relating to operational cooperation at Union level. We noted that we would look to ensure ENISA retained a supporting function but not a leading one in so that this does not impinge on the activities of national intelligence agencies and we are satisfied that the current version of the text makes this clear.

In our letter we also noted that we would look to ensure reassurance during the negotiations that the references to international standards are in line with global standards which are applied in an open and transparent way. We believe that the current references to standards are in line with these principles.

As noted in this correspondence we sought views from a wide range of stakeholders to help inform our position on the Regulation. The main themes of the feedback were: general support for ENISA's strengthened and permanent mandate, insistence on alignment with global standards, a call for further clarity on specific areas of the framework and for more industry involvement in the development of the schemes. We have found this feedback to be generally aligned with our negotiating position and have sought additional references to the involvement of industry in the creation of schemes.

Our remaining point of concern relates to the inclusion of three 'assurance levels' for all EU certification schemes - basic, substantial or high, which were defined as corresponding to a 'degree of confidence' in the cybersecurity qualities and described according to evaluation procedures. Our concerns have related to whether this would provide sufficient flexibility for the range of products and services and whether this would provide sufficient transparency of what security measures have been taken. In line with the Government's work on Secure by Design, we would prefer an approach which gives consideration to the processes by which internet connected products and services are developed.

Some measures have already been taken to increase the flexibility of this framework. We are continuing to work with Member States to develop an agreed approach in relation to the assurance levels to ensure adequate transparency and allow for methodology which tests for conformance against a secure by design approach.

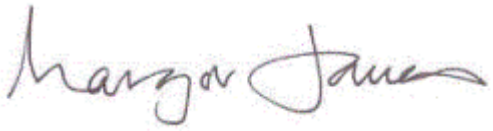
The Presidency's current intention is to raise this Regulation for a General Approach at the EU Telecomms Council on 8th June, although negotiations are ongoing within the Working Group and no agenda has yet been released. If there is a vote on these proposals at Telecomms Council on the 8th June, the Government's decision to vote in favour will be dependent on reaching a satisfactory compromise in relation to the points noted above on 'assurance levels'.

Request for Scrutiny Waiver

I hope this letter serves as a comprehensive update and that you can look to grant scrutiny clearance/waiver ahead of the Telecomms Council meeting on 8th June.

I am copying this letter to Lord Boswell, Chairman of the European Union Committee, Les Saunders, DExEU, Sarah Bailey and Agim Zekaj, DCMS.

Yours ever



MARGOT JAMES MP
Minister for Digital and the Creative Industries