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

Lord Boswell of Aynho
Chair of the European Union Committee
House of Lords
London
SW1A 0AA

TO2018/16580/DC
22 December 2018

Dear Tim

Thank you for your letter of 22nd November in response to my update on the proposed Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"). I last wrote to you on the 11th July to confirm the outcome of the UK's vote in favour of the General Approach for this file at Telecoms Council on 8th June. I am pleased to be able to provide a comprehensive update on trilogue discussions which have now concluded.

Five informal trilogues were held between 13th September and 10th December. At the last informal trilogue on 10th December an agreement was reached between the European Parliament and the Council.

As noted in my previous correspondence, there were many aspects where the European Parliament's proposed amendments aligned with the General Approach reached in the Council, including on industry involvement, self-certification, international standards and the importance of a process-driven approach. These were also aspects that the UK had successfully influenced and we therefore found to be positive developments. I have outlined below detail on the trilogue discussions on key areas where the Parliament's approach differed from the General Approach:

Part 1 - ENISA
The European Parliament proposed to include a role for ENISA in helping Member States to establish and **implement vulnerability disclosure policies.** This concept was welcomed by the Council with some amendments, including that it be on a voluntary basis. A recital was proposed to explain the concept and this explanation is compatible UK Government policy.

The Permanent Stakeholders' Group was renamed the "ENISA Advisory Group" as preferred by the European Parliament in order to differentiate between stakeholder groups. The Council was happy to compromise on this point, on which the UK did not hold strong views.

The European Parliament also expressed a preference for more regular cybersecurity exercises. Smaller Member States raised concerns about their capacity for this, whereas larger Member States including the UK were able to be more flexible. As a compromise which took into account those concerns about capacity, it was agreed to hold regular cybersecurity exercises with a large-scale exercise every two years. The UK was happy with this approach, which provides a balance and allows for some flexibility in regularity.

The area of most disagreement in relation to ENISA was on the role of ENISA in operational cooperation, with the European Parliament preferring a stronger role for ENISA. Some minor text changes were agreed in order to ensure ENISA had a clear and substantive role, but which still ensures the tasks remain in 'support' of operational cooperation among Member States, with technical support being at their request and information being analysed on the basis of voluntarily shared information. The UK was happy to agree to these small changes providing that they remained in support of Member State operational activity. We were aligned with a number of other larger Member States on this point.

Part 2 - Cybersecurity Certification

There were a number of discussions relating to the process by which a certification scheme can be developed and proposed. The European Parliament proposed that there be a **rolling work programme** published by the Commission which would identify strategic priorities for future European Cybersecurity Certification schemes. The Council, including the UK, assessed the general intention of these changes to be positive, as they provided additional clarity and we were content that the programme's proposed consultation process provided for sufficient industry input.

For schemes proposed outside of the rolling work programme, the European Parliament were not convinced that the **European Cybersecurity Certification Group (ECCG) should be able to request a scheme** directly to ENISA. While the UK was flexible on this point, there were a number of Member States who wished to maintain this. A compromise was reached on this point whereby in duly justified cases, the Commission or the ECCG may request ENISA to prepare a scheme outside the work programme.

The European Parliament also proposed that a **'Stakeholder Cybersecurity Certification Group'** be established to advise the Commission on strategic issues related to the Cybersecurity Certification Framework including the preparation of the rolling work programme. This would replace the certification advisory role which originally sat with the ENISA Advisory Group. For the development of schemes, the European Parliament proposed ENISA set up Ad Hoc working groups to provide tailored expertise. The UK was in support of these proposals, which would bring in additional industry expertise and it was agreed these should be included.

An article which would require the manufacturer or provider of certified products or services to provide **supplementary information** related to its cybersecurity was introduced. The concept was proposed by the European Parliament and acknowledged by the Council acknowledged as potentially adding value in providing the end user with awareness and trust. The Council and the European Parliament agreed a compromise which would provide for supplementary information which would be proportionate to the value and would not overburden businesses. The UK was content with this compromise, which allowed for greater flexibility in the method by which the information was provided and in the content.

The General Approach text in relation to **assurance levels** was broadly agreed to in its existing form in trilogues, acknowledging these were a result of lengthy technical discussions within the Council. It was very important to the UK to retain the compromises which had been reached during this time.

The most difficult discussions took place around the European Parliament's proposal that there be mandatory certification for operators of essential services under the NIS Directive. This was strongly opposed by a number of Member States including the UK. We had been supportive of the voluntary nature of the original proposals and were concerned that the mandatory certification proposal would be a disproportionate approach that could making those services more vulnerable as a result of lengthy certification processes. Our recommended approach was to wait until there was the necessary evidence to warrant mandatory certification and to consider what approach would be best in the context of specific schemes. A compromise was developed which allows for a future assessment to be carried out which would consider the merits of schemes in operation

and whether any shall be made mandatory through relevant Union legislation. We were therefore content to agree to such an assessment as a compromise.

The European Parliament and the Council both agreed to introduce the concept of **peer review.** There were some differences in relation to the scope and level of detail. The UK would have preferred to have this detail set out in the schemes. However, we were prepared to be more flexible on this point in order to seek concessions on the issue of mandatory certification. While the UK would prefer a Peer review mechanism which is less prescriptive than that proposed, it does not raise any major concerns.

On the main aspects of the proposals therefore, the UK is content that the compromises that have been reached continue to align with our principles of flexibility and proportionality; are open and transparent; in line with wider international standards and take account of industry expertise.

There is one outstanding point of concern for the UK. At a very late stage of the negotiations a proposal put forward by the European Parliament was adopted to include a task for ENISA to promote cyber security policies *'related to sustaining the general availability or integrity of the* ***public core*** *of the open internet'.*

The language 'public core (of the open internet)' originated in a report by the Global Commission on the Stability of Cyberspace relating to discussion of possible norms for state behaviour in cyberspace and was subsequently reflected in the Paris Call for Trust and Security in Cyberspace launched by President Macron at the Internet Governance Forum on 12 November 2018. The UK remains concerned about the use of the term 'public core' in this context which we consider is contrary to the multi-stakeholder model of internet governance and may undermine positions taken by the EU and Member States regarding avoiding fragmentation of the internet. Our signature to the Paris Call was made on the basis that the international community should work further towards appropriate language on this issue and that the Paris Call should not be considered legally binding due to these concerns.

While we gained some support from like minded Member States on this point, the European Parliament were not content to amend this language other than to include as part of the related recital a clarification that "*The* ***public core*** *of the open internet, meaning its main protocols and infrastructure, which are a global public good".*

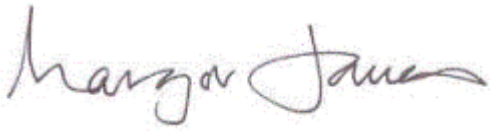
We would therefore seek to vote in favour of the Regulation, noting our overall support for the Regulation. However we will also look to include alongside our vote a Minute Statement, in order to put on record the UK's formal position in relation to the language on 'public core'.

If this Regulation comes into force before the UK leaves the EU on 29th March 2019, or within the Implementation Period if the Withdrawal Agreement is in effect from 29th March 2019, then it will have direct effect in UK law. We will need to take domestic legislative action to correct any deficiencies that may occur when it no longer has direct effect.

I hope that you will find this a comprehensive update and that you will be able to grant scrutiny clearance for the UK to vote in favour of this file. A vote is expected early January and so I would be grateful for urgent consideration of this.

I am copying this letter to Les Saunders from DExEU, James Ainsworth head of ongoing business at DCMS EU Team, Rachel Marnick scrutiny co-ordinator at DCMS EU Team, and Tristan Stubbs clerk in the EU Home Affairs Sub-Committee.

Yours ever



MARGOT JAMES MP
Minister for Digital and the Creative Industries