Department for Digital, Culture Media & Sport

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

020 7211 6000

www.gov.uk/dcms

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

TO2018/01006/DC
January 2018

Dear Bill,

Thank you for your response received on 7th December 2017 regarding the EMs about the Report from the Commission to the European Parliament and the Council on the evaluation of the Digital Single Market: ENISA / EU Cybersecurity Agency Regulation. I am grateful to the Committee for its consideration of these.

Your response seeks further clarification on a number of points. I have provided further detail on these points below:

- **"The Government previously told the Committee that it would 'challenge any proposals that seek to create EU-only standards, or standards where the associated conformity checking can only be performed by/under the control of European bodies.' We ask the Government to clarify whether, and to what extent, the Commission's proposal realises these concerns."**

The Government maintains that it is important to challenge proposals that seek to create EU-only standards in order to avoid market fragmentation both in the EU and globally. There are a number of ways in which the Commission's proposals refer to existing cyber security standards which are:

1. In broadening ENISA's mandate, it is provided with a number of additional tasks and functions. These include the development of policy and law and tasks relating to the market, cyber security certification and standardisation.
2. The proposed cyber security certification framework sets out the minimum content of what would be required under each scheme, including evaluation standards.
3. Conformity assessment bodies would be required to meet the requirements of global accreditation standards.

4. Supervision of conformity assessment bodies by national supervisory authorities would need to ensure conformity assessment bodies were meeting the requirements of global accreditation standards.

In our consideration of this text, we have been clear in our approach that we would seek to challenge those standards which were not global, open and transparent. The Commission specifies in the regulation that ENISA would facilitate the establishment and take-up of European and international standards. This has provided some reassurance that it is not their intention to create EU-only standards. We will seek to ensure during negotiations that ENISA's tasks would be conducted in line with global standards. This includes working with the Commission to ensure that those international standards are ones that have been developed globally, by global standards organisations and can be applied in an open and transparent manner.

In relation to the certification proposals, the Commission has again provided some reassurance by specifying in the text that the cyber security requirements of schemes within the framework are intended to be evaluated using international standards. The conformity assessment bodies who would certify products and services are also required to meet standards set by the International Organization for Standardization (ISO) and the national supervisory authorities would monitor and enforce this. Again, we will look to ensure reassurance during the negotiations that these standards are in line with global standards which are applied in an open and transparent way.

- "**Has the BSI been consulted in preparation of this Explanatory Memorandum? If so, what is its opinion of the Commission's proposed approach?"**

It is the Government's intention to consult with a wide range of industry stakeholders on the proposed Regulation, including the BSI, to inform its negotiation on the Regulation. As well as an online "call for views" which opened in December 2017, we intend this engagement to take place through roundtables and bilaterals throughout January 2018. We believe it is important that industry views are represented throughout the process. We are also aware that the BSI have been consulted through CEN/CENELEC as part of their coordinated response on the Commission's proposals.

- "**What scrutiny will there be by the Member States and the European Parliament of any Commission-developed implementing regulations which would create individual cybersecurity certification schemes that required the repeal of national schemes?"**

The Regulation sets out that when preparing certification schemes, ENISA would consult all relevant stakeholders and closely cooperate with the Group. The Group is composed of Member State national supervisory supervisory authority representatives. The Group's role in advising ENISA would include ensuring a consistent application of the framework and reviewing existing European certification schemes. The Regulation also provides for an evaluation and review of the certification provisions within five years, to assess the impact, effectiveness and efficiency. The results of this would be reviewed by the European Parliament, Council, Management Board and would be made public.

- **“The FCO expresses concern about prospective EU interference with national operational activities in the field of cybersecurity, whereas DCMS cautions that the Commission's use of the term "operational" to describe ENISA's proposed coordinating role in cross-border cybersecurity emergencies does not actually amount to an operational role in the UK usage of the term. What is the Government's considered view on this aspect of the proposal?”**

The proposed Regulation would give ENISA a permanent and strengthened mandate and as such sets out a number of renewed tasks and functions. This includes a number of tasks relating to operational cooperation at Union level. The main cause for concern is the description of these tasks as ‘operational’ as we would normally use operational in the context of national intelligence activities, which are the preserve of Member States. Some of the tasks detailed, in particular in preparing technical situation reports and providing technical assistance, could also be viewed as representing an extension of powers towards a more technical role, which again we would view as being the preserve of national intelligence agencies. Other large Member States share this concern and are likely to object to these provisions. However, from both the detailed text of the Regulation and the Commission’s own explanation, we do not believe that it is the intent that these tasks serve this function. Instead we believe their ambition is to actively increase cooperation and information sharing as part of their secretariat function. We will therefore work with the Commission and like-minded Member States so that ENISA retains a supporting function but not a leading one in operational cooperation so that this does not impinge on Member State competence.

- **The ENISA evaluation report concluded that ENISA's effectiveness had been hampered by its limited resourcing relative to its broad mandate. To what extent do the proposals reflect these findings? Is ENISA's mandate sufficiently reduced in scope in some areas to offset its new obligations? Alternately, is a major increase in resources proposed?**

In order to address the evaluation findings, the proposal sets out a renewed set of tasks and functions for ENISA in order to ensure it effectively and efficiently supports Member States, EU institutions and other stakeholders’ efforts to ensure a secure cyberspace. The scope of the mandate is delineated, strengthening areas where it has shown clear value and adding new areas where support is needed. The Regulation proposes that in order to guarantee the full autonomy and independence of the Agency and to enable it to perform additional and new tasks, it should be granted a sufficient and autonomous budget. It is proposed this will come primarily from the Union and from contributions from third countries participating in the agencies work. The Regulation also provides for the use of seconded national experts or staff not employed by the Agency. The UK view is that the proposed new set of tasks is ambitious when balanced against ENISA’s modest resources and therefore the practicality of these proposals will be further interrogated during the negotiation process.

- **“Regarding the Brexit implications of the proposal, we ask the Government to provide: A clear account of the means by which third countries currently participate in / cooperate with ENISA, including through the NIS Directive and its supporting institutional arrangements;”**

Article 30 of the current legislation which underpins ENISA (EU No 526/2013 of the European Parliament and of the Council of 21 May 2013) allows for the participation of third countries. It states that:

‘The Agency shall be open to the participation of third countries which have concluded agreements with the European Union by virtue of which they have adopted and applied Union legal acts in the field covered by this Regulation.

Arrangements shall be made under the relevant provisions of those agreements, specifying in particular the nature, extent and manner in which those countries will participate in the Agency’s work, including provisions relating to participation in the initiatives undertaken by the Agency, financial contributions and staff.’

The only third country to play an active role in the ENISA management board is Norway. Norway play an observer role at Management Board meetings attending on an ad hoc basis and holds no voting rights.

Under Article 13 of the NIS Directive it states that:

‘*The Union may conclude international agreements, in accordance with Article 218 TFEU, with third countries or inter-national organisations, allowing and organising their participation in some activities of the Cooperation Group. Such agreements shall take into account the need to ensure adequate protection of data.*’

Currently, Norway, Switzerland and the European Parliament have participated in NIS Cooperation Group Meetings.

- “ **A fuller account of the anticipated impacts of a shift to third country status for the UK and UK-based operators with regards to the main provisions of the ENISA Regulation and the NIS Directive (e.g., what would the impact be on digital service providers?);”**

The proposed new mandate for ENISA provides for continued participation between the Agency and competent authorities of third countries. It sets out that it may, subject to approval by the commission, establish working arrangements with the authorities of third countries.

Under the NIS Directive, third country status would impact on access to EU structures (the NIS Cooperation Group and the Computer Security Incident Response Teams (CSIRT), Network) and access to EU markets for Digital Service Providers (DSPs).

There is a provision in the NIS Directive to allow associate membership of the NIS Cooperation Group by third countries through a third country agreement. There is no equivalent provision for the CSIRT network. If the UK is considered a third country after the UK exits the EU then we would need to seek associate membership of the NIS Cooperation Group if we wanted to continue to participate in this group. If we wanted to continue to participate in the CSIRT network as a third country we would need to seek an alternative or bespoke solution to maintain access.

The NIS Directive states that any DSP established outside the EU, but which offers services within the EU must designate a representative in one of the Member States where they provide services and comply with the oversight of that Member State's competent authority. For the UK this means that post EU Exit, if the UK is considered a third country, all UK-established DSPs must designate a representative in another Member State if they want to offer services within the EU. They would then have to comply with that other Member State's security and incident reporting requirements, along with the UK's requirements (through our national implementation of the NIS Directive).

The Government will seek solutions to these two issues through its negotiations with the EU on the future EU/UK relationship.

- "**An explanation of the Government's concerns about the potential impact on trade and investment of the proposal for an EU certification framework, and how this might affect the UK when it assumes third country status;"**

A certification framework has the potential to negatively impact on trade and investment if it places unnecessary burdens on small business, if it does not align with global standards and therefore leads to market fragmentation or if it lacks openness and transparency which undermines trust.

However, the proposal as currently set out aims to build flexibility into the approach by setting out a framework under which schemes would operate, rather than setting out directly operational schemes. This allows schemes to be proportional to their need and protects the needs of small businesses. The proposal does outline the minimum content of what would be required under such schemes including; scope, objectives, categories of ICT products and services covered, detailed specification of the cyber security requirements, the specific evaluation criteria and evaluation methods, as well as the intended level of assurance. Where the certification framework sets out minimum content of schemes including evaluation standards - it makes reference to international standards. This gives us some assurance that ENISA will work to align with existing internationally recognised standards, which can be applied in an open and transparent way, in the development of certification schemes. This alignment will be important to avoid market fragmentation, both internally in the EU and globally and will protect against unnecessary barriers to trade and investment.

We will seek further clarification from the commission about how they intend EU certification schemes to interact with existing, more global schemes to ensure this does not result in fragmentation of the market. We would like to see more emphasis placed on alignment with global standards and will seek further reassurance from the Commission throughout the negotiation process that standards will be global, open and transparent and industry led. It is important that these changes do not result in a barrier for entry for companies wishing to deal in Europe after the UK exits the EU.

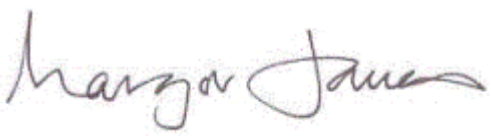
- **Clarification of whether, given that the UK may end up having to apply the EU acquis during a transitional / implementation period, (i) the Government shares the Committee's assessment that the JHA Opt-In Protocol does not apply, or (ii) if the Government disagrees, the factors it will take into account in deciding whether or not to opt into the proposed Regulation.**

The Government is of the view that the JHA opt-in does not apply in relation to the ENISA Regulation. The Regulation does not cite a Title V TFEU legal base and does not appear to contain JHA content. The purpose of the Regulation is to extend the mandate and remit of ENISA in its role of facilitating cooperation across the EU in matters of cyber-security and to set up a voluntary Cyber Security Certification framework. It does not seek to impose any requirements on the police or any other law enforcement agency. Although ENISA exercises functions which have a connection with JHA matters in that cyber-security is important in terms of protecting systems systems which support agencies which exercise functions in areas of JHA, this is only one of many areas that would be affected by a breakdown in cyber-security. The purpose of the Regulation is to maintain optimal cyber-security generally, rather than in areas of JHA specifically, and the Government therefore considers that the JHA opt-in does not apply.

I also note your request for an update of any progress that has been made in the Council. The EU Council negotiations on the proposal begun at an official level in October 2016 and have re-commenced under the new Bulgarian Presidency. The EU's current Action Plan for cybersecurity sites December 2018 as its aim for the negotiations to finalise. This is a more ambitious timetable than we had originally anticipated. We will continue to keep you updated on progress on the negotiations at the relevant points.

I am copying this letter to Lord Boswell, Tristan Stubbs in the Lords' European Union Committee, Kilian Bourke in the Commons' European Scrutiny Committee, Les Saunders in DExEU, Matthew Hull in DCMS and Agim Zekaj in DCMS.

Yours ever



MARGOT JAMES MP
Minister for Digital and the Creative Industries