**EXPLANATORY MEMORANDUM FOR EUROPEAN UNION LEGISLATION AND DOCUMENTS**

COM(2017) 477 FINAL
2017/0225 (COD)
12183/17

**PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON ENISA, THE "EU CYBERSECURITY AGENCY", AND REPEALING REGULATION (EU) 526/2013, AND ON INFORMATION AND COMMUNICATION TECHNOLOGY CYBERSECURITY CERTIFICATION ("CYBERSECURITY ACT")**

Submitted by DCMS on 18/10/2017

**SUBJECT MATTER**

The European Commission has proposed a Regulation on ENISA (previously the European Union Agency for Network and Information Security but now referred to as "the EU Cybersecurity Agency") and on Information and Communication Technology cybersecurity certification.

*ENISA's role and mandate*

ENISA's main task is to enhance capability to prevent and respond to network and information security problems within the EU by building on national and Union efforts. The five key activity areas as outlined in its strategy are (i) provision of expertise on network and information security issues, (ii) support to policy making and implementation, (iii) support for capacity building across the Union, (iv) to foster the network and information security community and to support Computer Emergency Response Teams (CERTs), and (v) to enable engagement with stakeholders.

ENISA has taken on specific additional roles and responsibilities in support of the implementation of Directive (EU) 2016/1148 on security of network and information systems (the NIS Directive). It now provides the secretariat to the Computer Security Incident Response Teams (CSIRTs) Network and assists the NIS Cooperation Group in the execution of its tasks and is intended to 'assist Member States and the Commission by providing expertise and advice and by the facilitation of best practice.'

ENISA is currently established under Regulation (EU) No 526/2013, which required the Commission to carry out an evaluation of ENISA before June 2018. This evaluation has taken place and its results are summarised in an accompanying Explanatory Memorandum. In that report the Commission states its intent to put forward a proposal to reform ENISA and provide it with a permanent mandate: this proposed Regulation constitutes that proposal and also outlines a role for ENISA in the delivery of a proposed cybersecurity certification scheme.

The proposed Regulation sets out a renewed set of tasks and functions for ENISA and aims to give it a stronger and more central role. Under the proposal ENISA would be granted a permanent mandate, though that mandate and its objectives and tasks would still be subject to regular review. The proposal strengthens and seeks to clarify ENISA's role as the EU Agency for cybersecurity and outlines its desire for ENISA to act as the central coordination point with all other relevant bodies. The proposed Regulation would make moderate revisions to the organisation and governance of the Agency, which were positively judged by the evaluation, to give greater consideration to the needs of 'wider stakeholders' in particular. The scope of the mandate is expanded in view of new EU policy priorities and instruments, in particular the NIS Directive, the EU Cybersecurity Strategy and the EU Cybersecurity Blueprint.

The proposal tasks ENISA with a role in the development and implementation of EU policy development and for it to play a specific advisory role. This would include the development and update of EU policy and law. This role goes beyond cybersecurity and states that ENISA would also support the development and update of EU policy and law in the areas of electronic communications, electronic identity and electronic verification services known as trust services in support of the delivery of cybersecurity.

ENISA would be tasked with contributing to the improvement of EU and Member State authorities' capability and expertise and to contribute to the establishment of information sharing and analysis centres. The proposal outlines a vision for ENISA to act as a knowledge and information sharing hub through the pooling of best practice from across the Union. Alongside this it is stated that ENISA should act as a point of guidance in the aftermath of cross border cyber incidents through the compilation of reports and guidance.

The draft Regulation proposes that ENISA should take on a role as a cybersecurity 'market observatory' by supporting EU policy development on standardisation, the development of standards and the promotion of the uptake of standards. This role would also cover the execution of the role of overseeing the EU framework for certification, the content of which is outlined below in more detail.

The proposal identifies a role for ENISA in the context of crisis management, including the delivery of an EU cybersecurity blueprint for the delivery of cooperation in emergency cybersecurity incidents. The word operational is used in this context though the detail of the text suggests that this is unlikely to constitute what the UK defines as a traditional operational role. This reference is likely to concern a number of Member States.

It is also proposed that ENISA could advise EU and national authorities on research and development priorities and the implementation of research and innovation EU funding programmes.

*Cybersecurity certification*

The Commission sets out an argument for the benefits of cybersecurity certification and its rationale as to why there should be a role for the EU in this space. It states that certification can play an important role in increasing the trust and security of products and services. The Commission considers that the current certification landscape is patchy and that as a result companies are required to undergo multiple

processes in order to offer products across EU Member States. They believe that this situation is resulting in higher costs and administrative burdens for companies who operate in multiple territories. The Commission believes that the continuation of this situation could damage the progress of the Digital Single Market.

This proposal sets out a framework which will 'govern' European cybersecurity certification schemes. It does not aim to introduce directly operational certification schemes but rather to create a system which will allow schemes to be established and recognised across the EU in order to address what it believes is an existing market fragmentation. The proposal outlines the minimum content of what would be required under such schemes.

As noted above the proposed Regulation specifies a role for ENISA in the delivery of this framework and notes that the schemes would be adopted by the Commission through implementing acts. It is stated that when the Commission identifies the need for a new scheme it will request that ENISA takes steps to prepare these schemes.

It is stated in the proposal that 'in order to ensure harmonisation' that on the adoption of this Regulation that national schemes would cease to apply and that no new national schemes should be developed at this point. On implementation the proposal suggests that manufacturers would be able to submit applications for certification to assessment bodies of their choice. The proposal does however place monitoring, supervisory and enforcement tasks with Member States. To deliver this Member States will have to provide for one certification supervisory authority. Alongside this the proposal also calls for the establishment of a European Cybersecurity Certification Group which would consist of all the national certification supervisory authorities and the secretariat for the group would be provided by ENISA. Its role would be to advise the Commission on issues concerning this field and to work with ENISA to develop draft schemes.

The Commission states that this proposal is consistent with associated policies such as the NIS Directive and the General Data Protection Regulation.

*Annex to the Proposal*

The Commission's annex to the Proposal sets out the requirements that bodies wishing to be accredited as conformity assessment bodies must meet.

**SCRUTINY HISTORY**

11013/16: Commission communication which set out a series of proposals designed to achieve greater pan-European co-operation in order to tackle the threat of cyber attacks and to support the growth of the cyber security industry, including the review of the mandate of ENISA.

6342/13: Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. This EM covered the proposal for a Directive which aimed to put measures in place in order to ensure a high level of network and information security across the EU in order to avert or minimise the risk of a major attack or technical failure of information and communication infrastructures in Member States. A supplementary EM was submitted on 13/03/16. This EM provided an overview and

analysis of the informal agreement reached by the Council and Parliament on the Network and Information Security (NIS) Directive in December 2015.

8104/16: Commission Communication on ICT Standardisation Priorities for the Digital Single Market. This EM covered proposed Commission activity on standardisation related to Information and Communication Technology (ICT) in the context of the Digital Single Market (DSM). This is part of a package of measures relating to digitising industry and DSM.

## MINISTERIAL RESPONSIBILITY

This proposal falls within the responsibility of the Secretary of State for Digital, Culture, Media and Sport. The First Secretary of State, the Foreign Secretary and the Secretaries of State for Business, Energy and Industrial Strategy, and for International Trade also have an interest.

## INTEREST OF THE DEVOLVED ADMINISTRATIONS

Telecommunications is a reserved matter under the UK's devolution settlements. However, the proposed Regulation may touch on sectors that are not reserved matters. The devolved administrations have been sighted on this EM for information and we will work with them on any devolved implications as we assess the policy proposals.

## LEGAL AND PROCEDURAL ISSUES

i. Legal basis
The legal basis for this proposed Regulation is Article 114 of the Treaty on the Functioning of the European Union (TFEU).

ii. European Parliament Procedure
The proposal is subject to the Ordinary Legislative Procedure.

iii. Voting procedure
The proposed Regulation will be subject to Qualified Majority Voting.

iv. Impact on United Kingdom Law
The proposed Regulation would be directly applicable in the UK. If adopted, the cybersecurity certification scheme may require legislation to be introduced to provide for a national certification supervisory authority. Where possible the UK will seek to adapt existing law.

v. Application to Gibraltar
This regulation will be applicable to Gibraltar to the extent that it relates to the provision of services.

vi. Fundamental rights analysis
We do not consider that the proposal raises any fundamental rights issues.

## APPLICATION TO THE EUROPEAN ECONOMIC AREA

The text is proposed to be relevant to the EEA.

**SUBSIDIARITY**

The Commission states that respect of subsidiarity of this area was recognised in the adoption of the current ENISA regulation. It states that to increase the collective cyber-resilience of the Union individual actions by EU Member States and a fragmented approach to cyber security will not be sufficient.

The UK Government remains of the view that a certain degree of voluntary EU coordination is beneficial in order to manage the cross-border context of cyber risks. The current flexibility in the text means that the Government is content that the proposed measures remain proportionate to the need. We will further consider our position on subsidiarity during the negotiation process.

**POLICY IMPLICATIONS**

On 23 June 2016, the EU referendum took place and the people of the United Kingdom voted to leave the European Union. The Government respected the result and triggered Article 50 of the Treaty on European Union on 29th March 2017 to begin the process of exit. Until exit negotiations are concluded, the UK remains a full member of the European Union and all the rights and obligations of EU membership remain in force. During this period the Government will also continue to negotiate, implement and apply EU legislation. The impact of the UK's departure from the European Union will be evaluated as part of the UK's negotiating position.

This regulation will propose giving ENISA a permanent mandate and a role in the development and implementation of the Union policy on cybersecurity certification. Officials will assess the policy implications during the negotiations, which the UK will take part in while it remains a member of the EU. Negotiations on the proposed regulation will commence at the end of October. They are unlikely to conclude before the UK leaves the EU in 2019. Alongside this the UK will need to enter into negotiations to agree its future relationship with ENISA after the UK leaves the European Union.

**CONSULTATION**

There is no consultation required on this Proposal or its Annex. The Commission conducted a public consultation for the review of ENISA pursuant to Regulation (EU) 526/2013.

**IMPACT ASSESSMENT**

An Impact Assessment (Staff Working Document) was carried out as part of the Commission's consultation on this initiative. This analysis led to the conclusion that a "reformed ENISA" together with an EU ICT cyber security certification framework were the most effective options to deliver the identified objectives. It proposes that the preliminary concepts be further assessed and evaluated with the Commission.

The UK Government will assess the need for an Impact Assessment or Checklist as it considers the policy implications.

**FINANCIAL IMPLICATIONS**

There will likely be some financial implications associated with the proposal on certification and these will be identified and evaluated as the negotiations progress. The Commission have articulated that they believe that the expanded role for ENISA specifically can be covered under current EU budgets directly rather than via requests for additional funding.

**TIMETABLE**

The Commission has not provided a clear timetable for the negotiations. We expect this regulation to be taken forward from the end of October. However, it is not clear that the Regulation will come into force before the United Kingdom leaves the European Union.

**THE RT HON MATT HANCOCK MP**
**MINISTER FOR DIGITAL**