

**From: Rachael Bishop, Department for Business Innovation and Skills**

## **NIS Directive**

### **Update on the negotiation**

The Council and the European Parliament started negotiating the text of the Directive in autumn last year. A number of areas have been informally agreed between the two institutions:

- Both Council and the EP would like to introduce more flexibility for Member States to use existing structures for the required 'institutional infrastructure' (e.g setting up CERTs). In particular, both institutions believe that Member States should be able to use existing/introduce sector-specific competent authorities to work directly with the affected operators and then nominate a single point of contact for any cross-border communications.
- Introducing criteria to allow Member States to develop sector-specific guidelines on what would constitute a reportable 'incident'. This would allow for national differences and differences between sectors.
- On cooperation, the Parliament has broadly accepted the Council preference for voluntary cooperation and information sharing. There will be a limited requirement to share information on incidents that would impact on the continuity of service in another Member State. EU CERTs will work together to draw up plans outlining how enhanced operational cooperation could work in the future.

There remain some differences between the Council and EP positions with regards to scope and cooperation on incidents:

- The main area yet to be resolved is the issue of scope (i.e. which companies should be covered by the Directive's requirements) where the concerns are twofold:
  - o First, for Council it is important that it is left up to Member States themselves to decide which companies are in scope of the Directive so that it is applied to those operators that provide critical services within the sectors identified in the Directive. The Parliament want to opt for a maximalist approach which would see all companies within the identified sectors included in scope which could represent an unjustifiable regulatory burden.
  - o Second, there has been no agreement on whether digital services (e.g. search engines, social media websites) should be in scope. Council remains divided on this question whereas the Parliament would like them to be excluded from scope. The negotiations between Council and Parliament have not yet touched on this issue in any detail.

## **Timing**

The negotiation could be resolved before the summer break but it is not inconceivable that it won't be agreed until autumn. Member States will then have two and a half years to implement the requirements into national law.

## **Background**

On 7 February 2013, the European Commission published a Directive on Network and Information Security (NIS). The proposed Directive aims 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.

The proposed Directive covers the following issues:

- Ensuring that Member States all reach a certain level of network and information security through obliging all Member States to produce a national cyber security strategy and establish points of contact for information sharing and cyber incident handling. It also mandates the establishment of 'competent authority' for cyber and a Computer Emergency Response Team ('CERT') in each Member State.
- Mandating information sharing between Member States, as well as establishing a pan-EU cooperation plan and coordinated early warnings and procedure for agreement of EU coordinated response for cyber incidents.
- Promoting the adoption of good risk management practices in the public and private sectors through the introduction of mandatory cyber incident reporting in various sectors similar to the obligations already apply to the telecoms sector.