EUROPEAN
COMMISSION

Brussels, 30.5.2016
COM(2016) 363 final

2013/0027 (COD)

**COMMUNICATION FROM THE COMMISSION
TO THE EUROPEAN PARLIAMENT**

pursuant to Article 294(6) of the Treaty on the Functioning of the European Union

concerning the

position of the Council on the adoption of a Directive of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union

(Text with EEA relevance)

2013/0027 (COD)

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT

pursuant to Article 294(6) of the Treaty on the Functioning of the European Union

concerning the

position of the Council on the adoption of a Directive of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union

(Text with EEA relevance)

1. BACKGROUND

Date of transmission of the proposal to the European Parliament and to the Council (COM(2013) 48 – 2013/0027/COD):	07.02.2013
Date of the opinion of the European Economic and Social Committee:	22.05.2013
Date of the position of the European Parliament, first reading:	13.03.2014
Date of adoption of the position of the Council:	17.05.2016

2. OBJECTIVE OF THE PROPOSAL FROM THE COMMISSION

First, the proposal requires all Member States to ensure that they have in place a minimum level of national capabilities by:

- establishing competent authorities for network and information security (NIS);
- setting up Computer Security Incident Response Teams (CSIRTs);
- adopting national NIS strategies and national NIS cooperation plans.

Secondly, the national competent authorities should cooperate within a network enabling secure and effective coordination, including coordinated information exchange as well as detection and response at EU level. Through this network, Member States should exchange information and cooperate to counter NIS threats and incidents on the basis of the European NIS cooperation plan. In order to ensure that all relevant authorities are duly and timely involved, the proposal also requires law enforcement agencies to be notified of incidents of a criminal nature and Europol to be involved in the EU-wide coordination mechanisms.

Thirdly, based on the model of the Framework Directive for electronic communications, the proposal aims to ensure that a culture of risk management develops and that information is shared between the private and public sectors. Companies in specific critical sectors and public administrations will be required to assess the risks they face and adopt appropriate and proportionate measures to ensure NIS. They will be required to report to the competent

authorities any incidents that seriously compromise their networks and information systems and significantly affect the continuity of critical services and the supply of goods.

3. COMMENTS ON THE POSITION OF THE COUNCIL

Overall the Council's position endorses the core objectives of the Commission proposal, namely to ensure a high common level of security of network and information systems. However, the Council makes a number of changes regarding how to achieve this goal.

National cybersecurity capabilities

Under the Council position, Member States will be required to adopt a national NIS strategy setting out the strategic objectives and appropriate policy and regulatory measures for cybersecurity. Member States will also be required to designate a national competent authority for the implementation and enforcement of the Directive, as well as Computer Security Incident Response Teams (CSIRTs) responsible for handling incidents and risks.

Although the Council position does not require Member States to adopt a national NIS cooperation plan, as envisaged in the original proposal, the position can be supported as some aspects of the cooperation plan are retained in the provision on the NIS strategy.

Cooperation between Member States

Under the Council position, the Directive will create a 'Cooperation Group' composed of representatives of Member States, the Commission and the European Union Agency for Network and Information Security ('ENISA'), to support and facilitate strategic cooperation and the exchange of information between the Member States. The Directive will also create a network of Computer Security Incident Response Teams, known as the CSIRTs Network, to promote swift and effective operational cooperation on specific cybersecurity incidents and the sharing of information about risks.

Though substantively different from the approach taken in the original proposal, the Council position can be supported as it corresponds overall to the objective of improving cooperation between Member States.

Security and notification requirements for operators of essential services

Under the Council position, 'operators of essential services' (equivalent to 'critical infrastructure operators' in the original proposal) will be required to take appropriate security measures and to notify serious incidents to the relevant national authority. However, the Council did not support an obligation for national competent authorities to notify incidents of a criminal nature to law enforcement authorities.

As per the original proposal, the Council position covers such operators in the energy, transport, banking, financial market infrastructures and health sectors. However, the Council position includes additionally the water and digital infrastructure sectors.

Member States will be required to identify these operators on the basis of certain criteria, such as whether the service is essential for the maintenance of critical societal or economic activities. Although this identification process was not part of the original proposal, it can be accepted given the Member States' obligation to submit to the Commission the information it needs to assess whether Member States are using consistent approaches to identify operators of essential services.

Public administrations as such are not included in the Council position. However, should they meet the criteria provided for under Article 5, they will need to be identified by Member

States as an operator of essential services, as operators of essential services may be public or private entities.

Security and notification requirements for digital service providers

Under the Council position, Member States will need to ensure that digital service providers (DSPs) take appropriate security measures and to notify incidents to the competent authority. The Council position covers online marketplaces (equivalent to e-commerce platforms in the original proposal), cloud computing services and search engines. Compared with the original proposal, the Council position does not include:

- internet payment gateways – these are now covered by the revised Payment Services Directive;
- application stores – these are to be understood as being a type of online marketplace;
- social networks – as per the Council's political agreement with the European Parliament.

Under the Council position, the Commission has been granted implementing powers for laying down procedural arrangements necessary for the functioning of the Cooperation Group as well as to specify further certain elements concerning DSPs, including the formats and procedures applicable to DSPs notification requirements.

The Commission supports the above outcomes.

Following the informal tripartite discussions on 14 October 2014, 11 November 2014, 30 April 2015, 29 June 2015, 17 November 2015 and 7 December 2015, Parliament and the Council reached provisional political agreement on the text.

This political agreement was confirmed by the Council on 18 December 2015. On 17 May 2016 the Council adopted its position at first reading.

4. CONCLUSION

The Commission supports the results of the inter-institutional negotiations and can therefore accept the Council's position at first reading.