High common level of network and information security across the Union. NIS Directive

2013/0027(COD) - 07/02/2013 - Legislative proposal

PURPOSE: ensure a high common level of network and information security (NIS) across the Union.

PROPOSED ACT: Directive of the European Parliament and of the Council.

PARLIAMENT'S ROLE: Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: network and information systems and services play a vital role in in facilitating the cross-border movement of goods, services and people. Substantial disruption of these systems in one Member State can affect other Member States and the EU as a whole.

The resilience and stability of network and information systems is therefore essential to the smooth functioning of the internal market.

The extent and frequency of security incidents, caused by human error or malicious attacks is increasing: the Commission's public consultation found that 57 % of respondents had experienced NIS incidents over the previous year that had a serious impact on their activities. A 2012 Eurobarometer survey found that 38% of EU internet users are concerned about the safety of online payments.

There is currently no effective mechanism at EU level for effective cooperation and collaboration and for secure information sharing on NIS incidents and risks among the Member States.

However, the Digital Agenda for Europe and the related Council conclusions highlighted the shared understanding that trust and security are fundamental pre-conditions for the wide uptake of information and communication technologies (ICT).

This proposal is presented in connection with the joint Communication of the Commission and High Representative of the Union for Foreign Affairs and Security Policy on a **European Cybersecurity Strategy.**

IMPACT ASSESSMENT: the Commission analysed three different options.

- ***Option 1***: **status quo**: maintain the current approach.

- ***Option 2:*** **regulatory approach**, consisting of a legislative proposal establishing a common EU legal framework for NIS regarding Member State capabilities, mechanisms for EU-level cooperation, and requirements for key private players and public administrations.

- ***Option 3:*** **mixed approach**, combining voluntary initiatives for Member State NIS capabilities and mechanisms for EU-level cooperation with regulatory requirements for key private players and public administrations.

The Commission concluded that **Option 2** would have the strongest positive impacts. The quantitative assessment showed that this option would not impose a disproportionate burden on Member States. The costs for the private sector would also be limited since many of the entities concerned are already supposed to comply with existing security requirements.

LEGAL BASIS: Article 114 of the Treaty on the Functioning of the European Union (TFEU).

CONTENT: the proposal aims to **effect a fundamental change in the way NIS is dealt with in the EU.** It provides for **regulatory obligations to create a level playing field** and close existing legislative loopholes. The objectives of the proposed Directive are as follows:

(1) To require all Member States to have in place a minimum level of national capabilities by establishing **competent authorities** for NIS, setting up **Computer Emergency Response Teams** (CERTs), and adopting **national NIS strategies and national NIS cooperation plans**.

(2) To ensure that the national competent authorities **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 will exchange information and cooperate, through the European Network and Information Security Agency (ENISA) to counter NIS threats and incidents and facilitate a uniform application of the directive throughout the EU.

(3) To ensure that a culture of risk management develops and that **information is shared between the private and public sectors.** Companies in the specific **critical sectors** – banking, stock exchanges, energy generation, transmission and distribution, transport (air, rail, maritime), health, internet services as well as public administrations will be required to:

- **assess the risks** they face and adopt appropriate and proportionate measures to ensure NIS;
- **report to the competent authorities** any incidents seriously compromising their networks and information systems and significantly affecting the continuity of critical services and supply of goods.

BUDGETARY IMPLICATIONS: cooperation and exchange of information between Member States should be supported by a **secure infrastructure**. The proposal will have EU budgetary implications only if Member States choose to adapt an existing infrastructure (e.g. sTESTA) and task the Commission to implement this under the Multiannual Financial Framework 2014-2020. The one-off cost is estimated to be **EUR 1 250 000** on condition that sufficient funds are available under the Connecting Europe Facility (CEF).

Alternatively, Member States can either share the one-off cost of adapting an existing infrastructure or decide to set up a new infrastructure and bear the costs, which are estimated to be approximately **EUR 10 million per year**.

DELEGATED ACTS: the proposal contains provisions empowering the Commission to adopt delegated acts in accordance with Article 290 of the Treaty on the Functioning of the EU.