EUROPEAN
COMMISSION

Strasbourg, 7.2.2013
SWD(2013) 31 final

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT

Accompanying the document

Proposal for a Directive of the European Parliament and of the Council

Concerning measures to ensure a high level of network and information security across the Union

{COM(2013) 48 final}
{SWD(2013) 32 final}

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT

Accompanying the document

Proposal for a Directive of the European Parliament and of the Council

Concerning measures to ensure a high level of network and information security across the Union

1. SCOPE

This impact assessment covers policy options to improve the security of the Internet and other networks and information systems underpinning services which support the functioning of our society (e.g. public administrations, finance and banking, energy, transport, health and certain Internet services enabling key economic and societal processes, such as e-commerce platforms and social networks). This issue is referred to as Network and Information Security (NIS).

2. POLICY CONTEXT

The increasing importance of NIS for our economies and societies was recognised for the first time by the Commission in 2001. In order to ensure a high and effective level of NIS in the EU the European Community decided in 2004 to establish the European Network and Information Security Agency (ENISA). The approach adopted so far by the European Union in the area of NIS has mainly consisted in the adoption of a series of action plans and strategies urging the Member States to increase their NIS capabilities and to cooperate to counter cross border NIS problems.

Stakeholders have been consulted on the different aspects of the initiative (problem definition and options to address existing shortcomings) through:

- An **online public consultation** on "Improving NIS in the EU" that ran from 23 July to 15 October 2012. A total of 169 responses were received via the online tool and a further 10 responses were received in writing by the Commission.
- Discussions with the **Member States** in the context of the European Forum for Member States (EFMS), in bilateral meetings and at the EU Conference on Cybersecurity organised by the Commission and the European External Action Service on 6 July 2012.
- Discussions with **private sector** companies and associations in the context of the European Public-Private Partnership for Resilience (EP3R) and in bilateral meetings.
- Discussions with **ENISA and CERT-EU**
- Discussions in the context of the **2012 Digital Agenda Assembly**

3. PROBLEM DESCRIPTION

3.1. Definition of the problem

The problem can be described as an overall ***insufficient level of protection against network and information security incidents, risks and threats across the EU undermining the proper functioning of the Internal market.***

Given that networks and information systems are interconnected and the global nature of the Internet, many NIS incidents transcend national borders and undermine the functioning of the Internal market.

Cross-border services can become unavailable, suspended or interrupted due to security breaches like in the attacks affecting eBay and PayPal. The need to act swiftly to remedy problems and to share information on a significant incident has been highlighted in the case of the attacks against Diginotar, the Dutch Internet certificate company. In the wake of past incidents Member States are starting to introduce their own regulations. Uncoordinated regulatory interventions may result in fragmentation and give rise to Internal market barriers generating compliance costs for companies operating in more than one Member State.

This problem affects all parts of society and economy (governments, business and consumers). In particular, a number of sectors play an essential role in providing key support services for our economy and society and the security of their systems is of particular interest to the functioning of the Internal Market. These sectors include banking, stock exchanges, energy generation, transmission and distribution, transport (air, rail, maritime), health, enablers of key Internet services and public administrations. The public consultation showed a strong support from stakeholders in addressing NIS in these sectors and to take action at EU level accordingly.

If no further measures are adopted to counter the increasing number of incidents, consumers' confidence in online services could suffer and this may undermine the achievement of the Digital Agenda objectives.

3.2. Drivers of the problem

The problem defined stems from a range of factors.

Firstly, there is an **uneven level of capabilities at national level across the EU**, which hinders the creation of trust among peers, which is a prerequisite for cooperation and information sharing.

Secondly, there is **insufficient sharing of information on incidents, risks and threats**. Most NIS incidents go unreported and unnoticed mainly due to the reluctance of companies to share this information because of fear of reputational damages or liability. Information exchange within the existing public-private partnerships/platforms, such as the EFMS and EP3R is limited to best practices.

4. EFFECTIVENESS OF EXISTING MEASURES

4.1. Loopholes in the existing regulatory framework

The current rules do not require entities other than telecommunication companies to adopt NIS risk management measures and report NIS incidents. However, all players relying on network and information systems face security risks. This leads to an uneven playing field since the same incident affecting for example a telecommunications provider and a company providing voice over IP services would have to be notified to the national competent authority in the former case, but not in the latter.

All players who are data controllers (e.g. a bank or a hospital) are obliged by the data protection regulatory framework to put in place security measures that are proportionate to the risks faced. But data controllers are required to notify only those security breaches compromising personal data.

Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures covers only the energy and transport sectors and to date only few European Critical Infrastructures have been identified as such by the Member States. The Directive does not put obligations on operators to report significant breaches of security and does not set up mechanisms for Member States to cooperate and respond to incidents.

The co-legislators are currently discussing the Commission proposal for a Directive on attacks against information systems[1]. This proposal covers only the criminalisation of specific conducts, but does not address the prevention of NIS risks and incidents, the response to NIS incidents and the mitigation of their impact.

4.2. The limits of a voluntary approach

The voluntary approach followed so far has resulted in an uneven level of preparedness and limited cooperation.

The EFMS has a limited remit given that the Member States do not share information on incidents, risks and threats nor do they cooperate to counter cross border threats. The EFMS has no power to require its members to have minimum capabilities in place.

ENISA has no operational powers and, for example, cannot intervene to fix NIS problems.

The EP3R has no formal standing and cannot require the private sector to report incidents to the national authorities. A framework for trusted information sharing and for communicating information on NIS threats, risks and incidents is absent within the EP3R.

5. NEED OF EU INTERVENTION, SUBSIDIARITY AND PROPORTIONALITY

Ensuring NIS is vital for the well-functioning of the internal market and the well-being of our society. Article 114 TFEU is an appropriate legal basis to harmonise NIS requirements and introducing a common minimum level of security across the EU.

Union intervention in the area of NIS is justified on grounds of **subsidiarity** due to the cross-border nature of the problem and the increased effectiveness (and thus add value) to existing national policies that would result from action at EU level.

In order to ensure cooperation encompassing all the Member States it is necessary to make sure that all of them have the required minimum level of capabilities. In addition, it is clear that concerted and collaborative NIS policy actions can have a strong beneficial impact on the effective protection of fundamental rights, and specifically the right to the protection of personal data and privacy.

The measures in the preferred option are justified on grounds of **proportionality** given that the requirements for the Member States are set at the minimum level necessary to achieve adequate preparedness and to enable cooperation based on trust and the requirements for businesses and public authorities to carry out risk management and to report incidents only target critical entities and impose measures that are proportionate to the risks and concern incidents with a significant impact. Furthermore, the measures under the preferred option would not impose disproportionate costs..

[1] COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF

6. OBJECTIVES

The general objective is to increase the level of protection against network and information security incidents, risks and threats across the EU. The specific objectives are:

- **Objective 1 -** To put in place a minimum common level of NIS in the MS and thus increase the overall level of preparedness and response.
- **Objective 2** - To improve cooperation on NIS at EU level with a view to counter cross border incidents and threats effectively.
- **Objective 3** - To create a culture of risk management and improve the sharing of information between the private and public sectors.

7. POLICY OPTIONS

The Policy options that have been considered in this Impact Assessment are: Business as usual, Regulatory approach and Mixed approach. The possible Option consisting of ceasing all EU activities on NIS has been discarded.

7.1. Option 1 – Business as usual ('Baseline scenario')

The Commission, with the assistance of ENISA, would continue with the current voluntary approach calling upon the Member States to set up NIS capabilities at national level (e.g. CERTs, national cyber incident/contingency plans, national cyber security strategies) and cooperate at EU level (e.g. via a network of CERTs across Europe and a European cyber incident contingency/cooperation plan).

7.2. Option 2 – Regulatory approach

The Commission would require all the Member States to set up at least a minimum level of national capabilities (CERTs, competent authorities, national cyber incident/contingency plans, national cyber security strategies).

Under this regulatory option, the national competent authorities and CERTs would be to be part of a **network** for cooperation at EU level. Within the network, the authorities and CERTs would exchange information and cooperate to counter NIS threats and incidents according to the **European cyber incident contingency/cooperation plan** on which the Member States would have to agree.

Companies (other than micro companies) in specific critical sectors, i.e. banking, energy (electricity and natural gas), transport, health, enablers of key Internet services and public administrations would be required to assess the risks they face and adopt appropriate and proportionate measures to dimension the actual risks. Moreover, these entities would be required to report to competent authorities those incidents seriously compromising the operation of their networks and information systems and thus having a significant impact on the continuity of services and supply of goods which rely on network and information systems. This scheme follows the one in Article 13a&b of the Framework Directive for electronic communications.

7.3. Option 3 - Mixed approach

The Commission would combine voluntary initiatives based on the goodwill of the Member States, aimed at setting up or strengthening Member States' NIS capabilities and at establishing mechanisms for EU-level cooperation, with regulatory requirements for key private players and public administrations.

Voluntary initiatives would in essence be similar to those undertaken under Option 1, whereas the regulatory requirements would be identical to those imposed under Option 2 both as regards the targeted entities and the substance of the obligations.

ENISA would provide support and technical expertise to the Commission, the Member States and the private sector, for example by issuing technical guidelines and recommendations.

8. ANALYSIS OF IMPACTS

The assessment covers, in addition to the level of security, the economic and social impacts of the three options. It covers also the costs which would be incurred under options 2 and 3.

None of the identified options will have impacts on the environment that can be predicted with accuracy.

8.1. Option 1 – Business as usual ('Baseline scenario')

Level of security: It is unlikely that all the Member States would reach comparable levels of national capabilities and preparedness necessary to improve security and enable cooperation and sharing trusted information at EU level. A level playing field would not be achieved with regard to risk management and increased transparency on incidents and regulatory loopholes would hence continue to exist.

Economic impacts: The impact would depend on the extent to which the Member States would follow the Commission's recommendations. The insufficient level of security in the less developed Member States would undermine their competitiveness and growth and expose them to risks and incidents. Given the current trends, NIS incidents would become more and more visible to business and consumers and hinder the completion of the Internal Market.

Social impacts: The continuation and expected aggravation of incidents, risks and threats would negatively affect the online confidence of citizens.

8.2. Option 2 – Regulatory approach

The level of security: The obligations placed on Member States would ensure that all of them are adequately equipped and would contribute to the creation of a climate of mutual trust, which is a precondition for effective cooperation at EU level.

The introduction of requirements to carry out NIS risk management for public administrations and key private players would create a strong incentive to manage and dimension security risks effectively. The total additional costs that would have to be borne across sectors in the EU to meet these requirements would be in the range from **1 to 2 billion EUR**. The compliance cost **per small and medium enterprise** would fall in the range of **2500 and 5000 EUR**.

Economic impact: As a result of the increased level of security financial losses associated with NIS risks and incidents would be reduced. Business and consumers' confidence in the digital world would be fostered and benefit the internal market. The promotion of an enhanced risk management culture would also stimulate demand for secure ICT products and solutions.

Social impact: A higher level of security would improve the on-line confidence of citizens who would be able to reap the full benefits of the digital world (e.g. social media, eLearning, eHealth).

8.3. Option 3 – Mixed approach

The level of security: As in Option 1, there is no guarantee that the level of security based on national NIS capabilities and cooperation at EU level would improve as a result of voluntary initiatives. On the other hand, the introduction of security requirements for public administrations and key private players would create a strong incentive to manage and dimension security risks. These mechanisms would however be ineffective in those Member States who would not follow the Commission recommendations on the setting up of NIS capabilities.

Economic impacts: The pace of development would vary significantly across the Member States. The insufficient level of security in the less developed Member States would undermine their competitiveness and growth and expose them to the negative impact of risks and incidents.

Social impacts: The continuation and expected aggravation of incidents, risks and threats would negatively affect online confidence, especially in those Member States which do not regard NIS as a priority.

9. COMPARING THE OPTIONS

Option 1 and 3 are not considered viable for reaching the policy objectives and are therefore not recommended, given that their effectiveness would depend on whether the voluntary approach would actually deliver a minimum level of NIS and, regarding Option 3, it would depend on the good will of the Member States to set up capabilities and co-operate cross-border.

Option 2 is the preferred one given that under this Option the protection of EU consumers, business and Governments against NIS incidents, threats and risks would improve considerably. Moreover, by putting its own house in order the EU would be able to extend its international reach and become an even more credible partner for cooperation at bilateral and multilateral level. The EU would hence also be better placed to promote fundamental rights and EU core values abroad.

10. MONITORING AND EVALUATION

Chapter 10 of the impact assessment report outlines a number of core indicators of progress towards reaching the objectives. These indicators include for example:

- For Objective 1, the number of Member States having appointed a NIS competent authority and a CERT or having adopted a national cyber security strategy and a national cyber incident contingency/cooperation plan
- For Objective 2, the number of Member States competent authorities and CERTs participating in the network and the volume of information exchanged within the network on NIS risks and incidents For Objective 3, the level of investments in NIS by key private players and public administrations and the number of notifications of NIS incidents with a significant impact