



Brussels, XXX
[...] (2012) XXX draft

COMMISSION STAFF WORKING DOCUMENT

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(2012) xxx}
{SWD(2012) xxx}

COMMISSION STAFF WORKING DOCUMENT

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**

TABLE OF CONTENTS

COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENTError! Bookmark not def

COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENTError! Bookmark not def

1.	Scope	6
2.	Procedural issues and consultation of interested parties	6
2.1.	Identification	6
2.2.	Organisation and timing	6
2.3.	Impact assessment process	10
3.	Policy context in the area of NIS	12
4.	Problem statement	12
4.1.	Problem definition: What is the problem?	12
4.1.1.	Disruptions to the EU internal market.....	12
4.1.2.	Rising number, frequency and complexity of NIS incidents, and incomplete view of their frequency and gravity	13
4.1.3.	Affecting all actors in the society and economy	15
4.1.4.	Sectors where the well-functioning of network and information security is key to preserve the well-functioning of the internal market	17
4.1.5.	What will happen if further measures are not adopted.....	19
4.1.5.1.	Undermined consumer confidence in the internal market	19
4.1.5.2.	Insufficient business investments in NIS	20
4.1.5.3.	Lack of credibility in the international scene	22
4.2.	Problem drivers: What is the reason behind the problem?.....	22
4.2.1.	Uneven level of capabilities across the EU	22
4.2.1.1.	Preparedness	24
4.2.1.2.	Response.....	24
4.2.2.	Insufficient sharing of information on incidents, risks and threats	25
5.	Effectiveness of existing measures	25
5.1.	There are loopholes in the existing regulatory framework	25
5.2.	The limits of a voluntary approach	27
5.3.	Approach in other regions of the world	28
5.4.	Need of EU intervention, subsidiarity and proportionality	31
5.4.1.	The EU right to act – Legal basis	31
5.4.2.	Subsidiarity test	32
5.4.3.	Proportionality of the approach	33

6.	Objectives.....	34
6.1.	Overview of general, specific and operational objectives.....	34
6.2.	Intervention logic	34
7.	Policy options	36
7.1.	Discarded Option.....	36
7.1.	Option 1 – Business as usual (‘Baseline scenario’)	36
7.2.	Option 2 – Regulatory approach	37
7.3.	Option 3 - Mixed approach	44
8.	Analysis of impacts	45
8.1.	Option 1 – Business as usual (‘Baseline scenario’)	45
8.2.	Option 2 – Regulatory approach	46
8.2.1.	Cost estimations	49
8.3.	Option 3 – Mixed approach.....	53
9.	Comparing the options	55
9.1.	Overall comparison of the assessment	55
9.2.	Overall cost-benefit analysis	56
10.	Monitoring and evaluation	58
ANNEX 1: PUBLIC CONSULTATION ON NETWORK AND INFORMATION SECURITY ACROSS THE EU		62
ANNEX 2: ACTION PLANS AND STRATEGIES ADOPTED SO FAR IN THE FIELD OF NIS IN THE EU		65
ANNEX 3: ASSESSMENT OF NIS RISK MANAGEMENT COMPLIANCE COSTS FOR PUBLIC ADMINISTRATIONS AND KEY PRIVATE PLAYERS.....		68
ANNEX 4: ASSESSMENT OF COSTS RELATED TO THE REQUIREMENT TO NOTIFY NIS INCIDENTS WITH A SIGNIFICANT IMPACT AND ASSOCIATED MECHANISMS/PROCESSES		91
ANNEX 5: THE SME TEST		Error! Bookmark not defined.
ANNEX 6: CURRENT STATE OF CAPABILITIES IN THE EU.....		96
ANNEX 7: INTERNATIONAL ORGANISATIONS AND BODIES DEALING WITH INTERNET/CYBERSECURITY.....		113
ANNEX 8: OVERVIEW OF CURRENT REGULATORY INCENTIVES FOR NIS IN THE SECTORS CONSIDERED FOR THE EXTENSION OF ART 13 TELECOM FWD IN OPTION 4 – REGULATORY APPROACH.....		117

ANNEX 9: EU EARLY WARNING AND INCIDENT HANDLING NETWORKS IN OTHER DOMAINS THAN NIS.....	125
ANNEX 10: COOPERATION FRAMEWORKS ESTABLISHED AT EU LEVEL FOR PREPAREDNESS AND RESPONSE TO CROSS-BORDER THREATS IN SPECIFIC AREAS	133
ANNEX 11: LEGAL AND REGULATORY ASPECTS OF INFORMATION SHARING AND CROSS-BORDER COLLABORATION OF NATIONAL/GOVERNMENTAL CERTS IN EUROPE.....	143
ANNEX 12: INTERNET 2011 IN NUMBERS	147
ANNEX 13: IMPACT ASSESSMENT MATRIX	152
ANNEX 14: LIST OF ACRONYMS.....	160

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).

Under Article 4(c) of Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency (ENISA): "network and information security" means the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems.

This impact assessment does not cover Member States activities concerning national security and defense.

2. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

2.1. Identification

Lead DG: Communications Networks, Content and Technology (CONNECT) Directorate General, former Information Society and Media (INFSO) Directorate-General.

Agenda planning: 2012/CNECT/003

2.2. Organisation and timing

The different aspects of the initiative have been discussed with a wide range of stakeholders. We have adopted an inclusive approach and respected the principles of participation, openness, accountability, effectiveness and coherence. The consultation included:

- Member States representatives responsible for enhancing the level of NIS and/or Critical Information Infrastructure Protection (CIIP). Discussions took place in the context of the European Forum for the Member States (EFMS) as well as in the form of dedicated meetings organised at the request of individual Member States. DG CONNECT received written inputs from 7 Member States.

A stocktaking exercise on the state of play of existing NIS capabilities and mechanisms in the Member States was carried out by Commission Vice-President (VP) Neelie Kroes via a letter sent to relevant Ministers in the Member States on 28 November 2011. Almost all the Member States took part in this exercise. A follow-up letter was sent by VP Kroes to the relevant Ministers following the Telecom, Energy and Transport Council of 8 June 2012.

Five Member States prepared a non-paper prior to the EU Conference on Cyber-Security that took place in Brussels on 6 July 2012 and that was jointly organised by the European Commission and the European External Action Service.

- **Private sector** representatives, including:
 - Individual electronic communications service and network providers, Internet service providers, and industry associations (e.g. ETNO, EuroISPA, EuroIX, etc.);
 - suppliers of hardware and software components for electronic communications networks and services, and industry associations (e.g. DigitalEurope, which represents large companies and SMEs);
 - providers of products and services for Network and Information Security;
 - representatives from the banking and financial sector and from the energy sector

Discussions with the private sector took place in the frame of the European Public-Private Partnership for Resilience (EP3R)¹, in the Expert Group on Security and Resilience of Communications Networks and Information Systems for Smart Grids² as well as in bilateral meetings. A number of relevant private sector players sent written contributions to the Commission.

- The **European Parliament**, in particular in the **Industry, Research and Energy (ITRE)** and **Security and Defence (SEDE) Committees**.
- The **European Network and Information Security Agency (ENISA)** and the Computer Emergency Response Team (CERT) for the EU institutions (**CERT-EU**).
- An online **public consultation**³ feeding directly into this impact assessment was open on the European Commission website from July 23 to October 15 2012⁴. A total of 169 responses were received via the online tool. A further 10 responses were received in writing by the Commission, bringing the total number of replies to the public consultation to 179. The public consultation focused on a) the scale of the problem and evidence of its impact b) options for improving NIS through an EU strategic approach c) options for improving NIS through risk management and reporting of incidents. A summary of the questions addressed and the answers received to the public consultation is provided in Annex 1.

The total breakdown by type of respondent is the following: 88 individuals (of which 57 intend to remain anonymous); 11 public authorities (of which 5 intend to remain

¹ The European Public Private Partnership for Resilience (EP3R) aims to foster the cooperation across Europe between the public and the private sector to develop coordinated strategic policy objectives as well as tactical/operational measures to strengthen security and resilience in CIIP

² http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/expert_group_smart_grid/index_en.htm

³ http://ec.europa.eu/information_society/digital-agenda/actions/infosec-consultation/index_en.htm

⁴ http://ec.europa.eu/information_society/digital-agenda/actions/infosec-consultation/index_en.htm

anonymous); 80 organisations or institutions such as businesses, research institutions and NGOs (of which 41 intend to remain anonymous). Amongst the companies that responded:

- 46% were large companies
- 20% were Small and Medium Enterprises (SMEs)
- 34% were micro enterprises
- A discussion with the **general public** was organised in the context of the 2012 Digital Agenda Assembly⁵.

An impact assessment Inter-Service Steering Group was set up. The following Commission services participated in the group: SG, SJ, DG AGRI, DG COMM, DG ESTAT, JRC, DG CLIMA, DG COMP, DG ECFIN, DG EAC, DG EMPL, DG MOVE, DG ENER, DG ENTR, DG ENV, DG SANCO, DG MARKT, DG HOME, DG JUST, DG REGIO, DG RTD, DG TAXUD, DG TRADE, DG BUDG, DG DIGIT, DG HR. The EEAS also participated in the group.

The Inter-Service Steering Group met four times: a kick-off meeting on 27 April 2012, a second meeting on 15 May 2012, a third meeting on 4 June 2012 to discuss the draft impact assessment report submitted on 13 June. A fourth meeting took place on 11 October 2012 to discuss the draft impact assessment report before re-submission on 15 October 2012. Before and after the meetings, written contributions and comments on the draft impact assessment were sent by the services.

The key questions addressed to the Member States and to the private sector in the context of all the relevant consultations listed above concerned the need to improve NIS across the EU. To this end, the Commission consulted on the need to foster cooperation at EU level; the importance of building up a minimum common level of national capabilities to enable such cooperation; the pros and cons of requiring the private sector to share information with the public sector and to adopt state-of-the-art protection measures; the establishment of such requirements at EU or national level.

Stakeholders' views on the seriousness of the problem and the options to address it are reported throughout this impact assessment where appropriate.

In general, the respondents to the public consultation:

- Expressed the view that governments in the EU should do more to ensure a high level of NIS (82.8% of respondents)
- Expressed the view that users of information and systems are unaware of the existing NIS threats and incidents (82.8% of respondents) and that businesses, governments and consumers in the EU are not sufficiently aware of the behavior to be adopted to minimize the impact of the NIS risks they face (84%).

⁵ Final report: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/daa12-final_report_1.pdf

- Would in principle be favourable to the introduction of a regulatory requirement to manage NIS risks (66.3% of respondents) at EU level (84.8% of those respondents).
- Expressed the view that it would be important to adopt NIS requirements in particular in the following sectors: banking and finance (91.1% of respondents), energy (89.4%), transport (81.7%), health (89.4%), Internet services (89.1%), public administrations (87.5%).
- Expressed the view that requirement to adopt NIS risk management according to the state of the art would entail for them no additional significant costs (43.6%) or no additional costs at all (19.8%).
- Expressed the view that if a requirement to report NIS security breaches to the national competent authority were introduced, it should be set at EU level (65.1%) and affirmed that also public administrations should be subject to it (93.5%).
- Affirmed that a requirement to report security breaches would not cause significant additional costs (52.5%) and 19.8% said that it would not cause additional costs at all.

In the EFMS and in written inputs to the Commission, the Member States expressed the following views:

- The Commission should develop current NIS actions and mechanisms (Germany, France) especially by means of targeted binding measures (France)
- The development of cyber-security capabilities should be accelerated within the Member States, particularly within the least advanced ones (France)
- That NIS protection levels vary across Europe (Germany) and that there are no mechanisms for engaging in existing cooperation mechanisms with those Member States who are less active in NIS nor are there paths for these Member States to get involved (Estonia).
- An EU framework establishing mechanisms for cooperation on preparedness and response amongst the Member States should be set up (France, Romania, Estonia, Germany, and Finland). In particular:
 - Cooperation between the Member States should be underpinned by confidentiality agreements and mechanisms to exchange sensitive data (Spain, Romania).
 - Information exchange on good practices and expertise; early warning and crisis management including via cyber-incident exercises should be promoted (Germany, Finland).
 - Cooperation should be built on mutual trust (Germany, Finland).

- A functional and effective network of national/governmental CERTs in Europe in which information is exchanged according to the necessary confidentiality standards is needed (France, Romania).
- An approach focused on preparedness and prevention should use harmonized requirements regarding minimum security standards across the EU by maintaining the conditions for fair competition (Germany)

Moreover, the Member States:

- Expressed support for considering the extension of the security provisions in the regulatory framework for electronic communications to new sectors (France) with the appropriate involvement of the Member States in the related discussions (such discussions took place already within the EFMS)
- Expressed support for an EU initiative on NIS covering the ICT sector but also, in a horizontal manner, the ICT component virtually underpinning all sectors (Germany)
- Expressed support for the development of a risk management culture in the private sector (Germany).

The UK questions the merits of a regulatory intervention on NIS at EU level and favours a voluntary cooperation approach facilitated by the Commission. It has particular concerns about the extension of mandatory reporting requirements to sectors other than telecoms.

The **European Parliament Resolution** of 12 June 2012 on "Critical Information Infrastructure Protection: towards global cyber-security⁶" recommends the Commission to:

- "Propose binding measures via the EU cyber incident contingency plan for better coordination at EU level of the technical and steering functions of the national and governmental CERTs";
- "Propose binding measures designed to impose minimum standards on security and resilience and improve coordination among national CERTs"
- "Propose an EU framework for the notification of security breaches in critical sectors such as energy, transport, water and food supply, as well as in the ICT and financial services sectors, to ensure that relevant Member State authorities and users are notified of cyber incidents, attacks or disruptions"

2.3. Impact assessment process

A first version of this impact assessment report was submitted on 13 June to the European Commission Impact Assessment Board and discussed at a meeting convened

⁶ <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167>

on 5 July 2012. A revised version of the impact assessment was submitted on 15 October. This new version took into account the various comments from the Board , in particular: a better explanation of the relation between the problem and its cross-border dimension (Chapters 4 and 5); the insufficiency of existing policy measures to solve the problem; the integration of stakeholders' views on various aspects of the problem statement and on all key points of the preferred option; the identification of the sectors and players that would be covered by the preferred option (Chapter 7) and an estimation of the corresponding costs (Chapter 9 and Annexes 2 and 3) that highlighted with more precision the proportionality of the preferred option.

Following the opinion of the Board of 24 October, the following further amendments were made to this impact assessment:

- Insertion of a table showing the extent to which existing obligations address NIS issues and the gaps that still need to be addressed.
- A better explanation of the lack of motivation and incentives for companies and the public sector to invest in NIS (Section 4.1.5.2).
- A description of the nature of the risks in the sectors covered including the extent to which and how networks and services may be affected (Section 4.1.4); strengthening the evidence base and better explaining the rationale for the choice of the relevant sectors in the preferred option (Section 4.1.4).
- Additional details on the content of the preferred option (Option 2) and in particular on what NIS risk management requirements would entail in practice (Section 7.2).
- A better explanation of the reasons for not considering other combinations of "soft" and "regulatory" approaches (Section 7.3)
- Improved assessment of social/employment impact, on competitiveness in particular for the preferred option, impact on international cooperation (Section 8 on Assessment of impact of the Options).
- A description and rough estimate of the benefits (i.e. decreasing the cost of NIS incidents and the improved level of security) (Section 9)
- Insertion of a summary table of all costs and benefits per option (Section 9).
- Insertion of a summary of the questions asked and of the responses received in the public consultation (Annex 1).
- Inclusion of the views of stakeholders throughout the text and in the preferred Option.
- Inclusion of the indication of the tools for monitoring and evaluation (Section 10).

3. POLICY CONTEXT IN THE AREA OF NIS

The increasing importance of NIS for our economies and societies was recognised for the first time by the Commission in a Communication from 2001⁷.

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.

Annex II provides a description of the "Action plans and strategies adopted so far in the field of Network and Information Security in the EU".

Companies, with the exception of telecommunication operators ('undertakings providing public communications networks or publicly available electronic communications services'⁸) and public administrations are not subject to NIS requirements and are not required to report security incidents⁹.

4. PROBLEM STATEMENT

4.1. Problem definition: What is 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*. The problem is further detailed in the following sections.

4.1.1. Disruptions to the EU internal market

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

The effects of an incident originating in a particular country, if not appropriately contained, may spread quickly to other countries. Even, incidents that are local by nature may have unforeseen consequences across borders, e.g. the disruption to a major airport's IT systems may affect air traffic across Europe.

Cross-border services can become unavailable, suspended or interrupted due to security breaches. eBay has experienced web-based attacks that have made all or portions of its websites unavailable for periods of time in 2010 and likewise PayPal¹⁰, thereby affecting e-commerce in the internal market.

The case of Diginotar illustrates the risks posed by not reported security breaches. The Dutch certification company Diginotar did not report that its systems were hacked and

⁷ COM(2001)298

⁸ See

http://ec.europa.eu/information_society/policy/ecomms/doc/library/regframeforec_dec2009.pdf

⁹ These consisted of security provisions including on security breaches notifications (Art. 13a&b of Framework Directive 2002/21/EC), and were to be transposed at national level by 25 May 2011

¹⁰ eBay Inc. filing to SEC for the fiscal year that ended 31.12.2010
<http://www.sec.gov/Archives/edgar/data/1065088/000106508810000003/ebay10k20101231.htm>

did not revoke the digital certificates (i.e. the certificates ensuring the security of communications over the Internet) that were fraudulently issued. This resulted in a large number invalid certificates circulating online, compromising the security of Internet services and eventually affecting trust in the Internet. A report¹¹ by the security firm Fox-IT, which investigated the case, found out that there were a number of problems in the security practices of the company, revealing the need for better risk management and mitigation practises. It must be borne in mind that in the aftermath of the Diginotar incident, the Dutch Government acknowledged that "the risk of security breaches affects the internal market [...and] hampers cross-border services and product supplies". For this reason the Dutch Government is preparing a system of mandatory security breach notifications for relevant critical infrastructure and national services¹².

In January 2011, the Commission had to suspend trading in the Emissions Trading System due to security breaches at national registries¹³ and companies were prevented from selling and buying emission allowances within the EU.

In the wake of past incidents Member States are starting to introduce their own regulations. As already remarked, the Netherlands are considering introducing security breach notification requirements and Luxembourg¹⁴ has introduced a disclosure requirement for incidents that can have financial consequences for the companies concerned. The UK has taken a sector-specific approach to put in place reporting requirements for critical sectors such as finance, energy, transport and health. 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 States.

Those businesses which replied to the public consultation emphasised the role that the EU could play in creating a truly integrated and harmonised internal market for NIS products and services and the existence of market barriers which undermine cybersecurity across the EU.

4.1.2. Rising number, frequency and complexity of NIS incidents, and incomplete view of their frequency and gravity

The availability, authenticity, integrity and confidentiality of information and networks can be compromised due to various causes, such as natural events, human errors or malicious attacks.

The outcome of the public consultation confirms the seriousness of the problem, in particular:

¹¹ <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf>

¹² http://nctb.nl/Images/brief-cyber-meldplicht-en-interventie_tcm91-435018.pdf
<http://nctb.nl/Actueel/Nieuwsberichten/2012/wettelijke-regeling-meldplicht-en-interventiemogelijkheden-bij-digitale-veiligheidsincidenten.aspx?cp=91&cs=25481>

¹³ <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/34>

¹⁴ Circular CSSF 11/504 – Frauds and incidents due to external computer attacks

56.8% of the respondents reported having experienced over the last year NIS incidents (caused by human mistakes, natural events, technical failures or malicious attacks) which have had a serious impact on their activities.

27.8% of the respondents to the public consultation affirm that human/technical errors are very frequently the cause of NIS incidents, and 39.6% affirm that this is the case quite frequently.

40.8% of the respondents to the public consultation affirm that malicious attacks are quite frequently the cause of NIS incidents.

36.1% of the respondents to the public consultation affirm that software/hardware failure is quite frequently the cause of NIS incidents.

47.3% of the respondents to the public consultation affirm that third party/external failure is quite frequently the cause of NIS incidents.

The flooding of the river Elbe in 2002¹⁵ illustrates how communications systems can be disturbed by a natural disaster. Human error or ignorance can also be the cause of cyber incidents by leading to accidental events. In August 2012 a sub-sea cable was mistakenly snapped between the UK and the Netherlands causing certain Internet Service Providers, e-commerce service providers and customers to be cut off the Internet for more than 24 hours¹⁶. Incidents of this kind (cable cuts) had already happened in the Mediterranean in 2008 and in the Suez canal in 2011.

The human factor is of the utmost importance for NIS. Non-compliance with security requirements (e.g. by negligence or distraction, using infected USB sticks, opening unsolicited e-mails, failing to apply security patches or revealing passwords) can cause an outage or facilitate the intrusion of malicious software.

The spread of malicious software (malware) and malicious attacks have been increasing steadily. Web based attacks increased by 36% in 2011 compared to 2010 and the total number of attacks by 81%. Malware can mutate as they spread, and attackers are able to generate an almost unique version of their malware for each potential victim¹⁷, which makes their detection ever more challenging. Figure 1 shows the raise in the number of incidents reported to the US-CERT in 2006-2011.

¹⁵

http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/Leitfaden_Schutz_kritischer_Infrastrukturen_en.pdf?__blob=publicationFile

¹⁶

http://www.theregister.co.uk/2012/08/28/cut_underseas_cable_cripples_networks/?utm_source=google&utm_medium=twitter&utm_campaign=Feed%253A+InformationSecurityDisclosure+%2528Information+Security+Disclosure%2529

¹⁷

Internet Security Threat Report Volume 16, Symantec

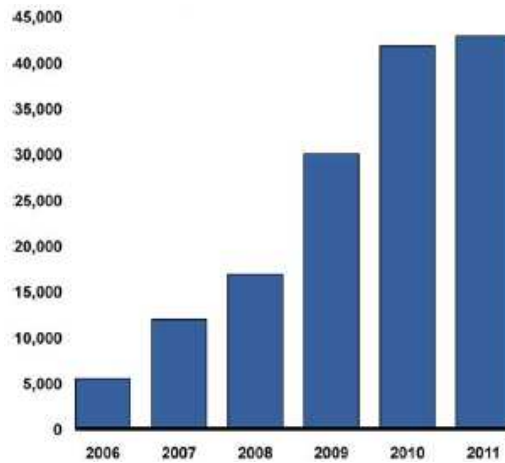


Figure 1: Incidents reported to US-CERT: Fiscal Years 2006-2011¹⁸

In addition to the elements presented above, there is reason to believe that a large proportion of attacks go unnoticed. The recent outbreak, in late May 2012, of the ‘Flame’¹⁹ cyber-spying software, revealed that malware can be spreading undetected over a number of years. There is moreover reason to believe that only a fraction of incidents, when discovered, are disclosed. The reluctance to disclose comes from the potential significant damages for the organizations involved, including reputational damages and loss of business opportunities.

The lack of information on incidents slows down the capability to react and take the appropriate mitigating measures, in particular in cases where the incident has repercussions outside the organisation and the other parties affected are unaware of an imminent threat or an incident/intrusion that has already taken place.

The most serious of these cross-border incidents may be the state-sponsored stealthy attacks such as ‘Shady Rat’ etc.²⁰, where the same techniques are applied in one country then another. Trusted sharing of information about such attacks could help prevent attacks spreading to further countries.

4.1.3. *Affecting all actors in the society and economy*

Over the last decade, the digital ecosystem has become essential to economic growth and societal welfare. It has enabled the creation of high-quality jobs and supported smart and sustainable economic growth.

Indeed, the ICT sector is one of the growth engines of the EU. In Europe, the ICT sector and investments in ICT deliver around half of our productivity growth. The World Bank estimates that with 10% increase in high speed Internet connections, economic growth would increase by 1.3%. The ICT sector alone represents almost 6% of the European GDP²¹.

¹⁸ Cybersecurity, Threats Impacting the Nation, GAO 2012

¹⁹ <http://www.enisa.europa.eu/media/news-items/The-threat-from-Flamer.pdf>

²⁰ <http://www.eweek.com/c/a/Security/Huge-Shady-RAT-CyberAttack-Likely-Targeted-Thousands-More-Victims-503656/>

²¹ The Internet economy has generated 21 % of the GDP growth of the last 5 years and could represent as much as 20% of GDP growth in the period up to 2015 in the Netherlands and in the

Public administrations, businesses and consumers reap huge economic and social benefits from the usage of ICT, including online services. Because of the critical role of networks and information systems, possible failures or attacks could impact all parts of society – Member States/governments, organisations/business and citizens/consumers.

Security incidents are capable of rendering critical **government functions** unavailable for several days, as demonstrated by the cyber-attacks against Estonia in 2007, which severely affected not only the provisioning of online services such as e-government and e-banking within the country, but also prevented citizens from accessing online services across borders. **EU institutions** have been the target of attacks in 2011 and 2012.

Businesses and other organisations can be seriously affected if the networks and information systems underpinning their industrial processes are compromised. In 2009, 16 % of enterprises in the EU-27 had experienced some kind of NIS incident²². Incidents can be costly. The cyber-attacks targeting Sony in April 2011 cost the company nearly \$175 million²³. An outage that affected BlackBerry in 2011 cost the company \$50 million²⁴. Beginning in July 2009, two U.S. stock exchanges were victims of cyber-attacks²⁵. The remote attack temporarily disrupted public websites. In September 2012, six major US banks were hit by cyber-attacks²⁶. The loss of intellectual property, trade secrets and financial data ensuing from cyber-attacks also result in considerable losses for businesses concerned. The UK estimates the loss of intellectual property to be largest cost category, accounting for 30% of total losses, resulting from illegal intrusions and cyber-crime, with identity theft and loss of customer data accounting for a much smaller proportion of losses²⁷.

Consumers can face interrupted e-mailing, instant messaging and browsing services, as it was the case in October 2011, when BlackBerry handsets were affected by a network outage at one of its data centres in the UK and almost all of its 70m users worldwide experienced problems at some point during the three days that the incident lasted²⁸. In January 2010, German card holders were suddenly unable to conduct banking or ATM withdrawals and purchases with their bank cards both at home and abroad, due to

UK. Internet consumption and expenditure already exceed the share of GDP of agriculture or energy, and its GDP is bigger than the GDP of Canada or Spain. It represents 7% of UK GDP, 3.7% in France, 2.2% in Spain, 2% in Italy, 2.7% in Poland, 3.6% in the Czech Republic, 4.3% in the Netherlands, 5.8% in Denmark, 6.6% in Sweden, 3.4% in Germany and 2.5% in Belgium. According to IMRG, in March 2010, 600,000 jobs were associated with e-commerce in the UK.

Each year, 200 million Europeans – 40% of all citizens – buy over the Internet. 27% of European enterprises purchase and 13% sell online. Some sectors have already been profoundly transformed by e-commerce. These include travel agencies (39% of sales took place online in 2008), sales of electronic and cultural goods (22%), financial services, gambling and sports betting (5th Consumer Scoreboard - March 2011).

²² Source, Eurostat, http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cisce_ic&lang=en
²³ <http://www.sec.gov/Archives/edgar/data/313838/000115752311003320/a6733820.htm>

²⁴ <http://www.sec.gov/Archives/edgar/data/1070235/000107023511000054/pr120211.htm>

²⁵ Source, FBI, Statement before the House Financial Services Committee, <http://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector>

²⁶ http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html?_r=0&adxnnl=1&adxnnlx=1349785139-tC3YxWCWhVImONk4tIKGZA

²⁷ A Detica Report, in partnership with the Office of Cyber security and information assurance in the UK Cabinet Office, 2012 "The cost of cyber-crime".

²⁸ <http://www.rim.com/newsroom/service-update.shtml>

software problems in the microchips. In the EU, nearly one third of users have already been confronted with a computer virus (or similar infection). Also, 74% of EU Internet users in 2012 think that the risk of becoming a victim of cybercrime has increased in the past year²⁹. **82.8% of respondents to the public consultation expressed the view that users of networks and information systems are not sufficiently aware of the level of NIS threats and incidents 84% of the respondents affirmed that businesses, governments and consumers in the EU are not sufficiently aware of the behavior to be adopted to minimize the impact of the NIS risks they face.**

4.1.4. Sectors where the well-functioning of network and information security is key to preserve the well-functioning of the internal market

While the problem described above affects all actors of society and economy in the EU, a number of sectors and a number of infrastructure and service providers in those sectors are particularly vulnerable, due to their high dependence on correctly functioning network and information systems and due to their essential role in providing key support services for our economy and society, including health, safety, security and the economic and social well-being of people. As a result, the security of their systems is of particular interest to the functioning of the Internal Market.

The public consultation underlined the importance of ensuring the security of network and information systems, in particular for the following sectors:

- Energy – 89.4% of respondents
- Transport - 81.7% of respondents
- Banking and finance – 91.1% of respondents
- Health – 89.4% of respondents
- Internet services – 89.1% of respondents
- Public administrations – 87.5% of respondents

At the same time, **31% of respondents (both business and consumers) to the public consultation affirmed to have no process in place to manage NIS risks. Also, 54.2% affirmed not to have any budget dedicated to NIS.**

All the sectors, which provide services which are key for the functioning of our economies and well-being of our society, rely heavily on network and information systems.

Banking activities should be secured since banks are the backbone of our financial system and because they are common targets of fraudsters. Indeed there are signs that attacks are increasing in this sector. McAfee reported recently³⁰ that fraudsters, using malware, and replicating the same scheme in several countries, have attempted to steal up

²⁹ Special Eurobarometer 390/2012 on cyber security
http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf
³⁰ <http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf>

to €2 billion from accounts in Europe, the United States and Columbia. Consumers and businesses using online banking have increasingly experienced theft, particularly through viruses infecting their computers. Especially in this sector, we observe an increasing usage of third party business applications (such as those used for mobile banking). These applications, which are often cloud-based, are not part of the network and systems of the credit institution, which has no control over their security.

The stock exchange increasingly adopts networks and information systems and Internet-based commerce systems. Accidental disruptions or malicious attacks affecting the stock exchange in a country or affecting particularly critical stock exchanges such as the ones in London, Paris or Milan may have very significant impact on trade both in the internal market and internationally. In 2010 the London Stock Exchange experienced a serious cyber-attack at its headquarters, which compromised its trading system³¹.

Generation, transmission and distribution of energy are highly dependent on secure network and information systems. Ensuring the resilience of utilities is particularly important since virtually all other sectors and the well-being of our society depend upon them.

For example, many major gas companies suffer increased amounts of cyber-attacks motivated by commercial and criminal intent. These attacks are posing a great risk to machinery, which can cost lives, stop production and cause environmental damage.

The same considerations are valid for other network industries, such as air, maritime transport and railways and for key transport infrastructure, such as airports, ports, railways, and traffic management systems and logistics. For example, aviation infrastructure (including ground and in-flight Air Traffic Management) relies on continuous and uninterrupted information flows and databases, which cannot be allowed to fail. Airports and border gateways are dependent on information assurance regarding data, control systems, networks and protocols that support the effective functioning of aviation³².

Both the energy and the transport sector heavily rely on Industrial Control Systems (ICS), i.e. complex computer and information systems that can be located either in one site (e.g. power plants) or distributed over a geographical area (energy and transport networks).

There are numerous interconnection points between ICS, including over the Internet, and securing them is of the essence. Also, many ICS were designed in the past without anticipating the security threats posed by technological advancements. For example, remote controlling of ICS is often done via simple laptops or other mobile devices which may have a lower level of security than the rest of the system.

The Expert Group on Security and Resilience of Communications Networks and Information Systems for Smart Grids recently concluded that "Electricity Critical infrastructures converging with ICT-infrastructure require scenario-building that includes consideration of highly unlikely types of events. ICT security considerations need to be integrated within the wider risk management of the whole grid. ICT is

³¹ <http://www.cio.co.uk/news/3258814/london-stock-exchange-under-major-cyberattack-during-linux-switch/>

³² Source: Centre for Strategy and Evaluation Services, Interim Evaluation of FP7 Research activities in the field of Space and Security, http://ec.europa.eu/enterprise/policies/security/files/doc/aviation_case_study_csese_en.pdf

therefore needed to carry out a risk analysis, and to define high level security requirements to enhance the security and resilience of ICT for Smart Grids."³³

Hospitals and clinics are becoming the more and more reliant on sophisticated ICT systems which need to be secure to ensure continuity of service and avoid fatal disruptions. The proliferation of electronic medical devices presents unique challenges in ensuring that only known, authorized devices are able to connect to the network.

Also, personal health and financial information is often target of cybercrime, particularly as the healthcare industry continues its conversion process to full patient electronic medical records. Networks, mobile devices, workstations, servers and medical devices are particularly critical in this regard and securing them is of the essence.

It is important to ensure the security of Internet companies (e.g. cloud providers, social networks, e-commerce platforms, search engines), which provide key inputs enabling important economic and societal processes. This is essential to preserve trust in the digital ecosystem.

It is key to ensure the resilience and reliability of public on-line services to citizens to build and preserve their trust in e-government. E-Government and e-participation are increasing with citizen demand for timely and cost-effective services and so are the NIS risks for state and local administrations. The risk for public online services to be hindered by NIS problems exist at all levels of government.

Finally, there are NIS problems that are common to all the sectors referred to above. For example, malware is one of the most significant threats as it may disable security or other software in an organisation and cause a breach or a gap that can be exploited by external parties. Also, exposure to threats grows as companies and public administrations invest in technologies like mobile, social, and cloud. Notably, due to the increasing use of mobile devices and applications, employees in virtually all sectors can now access corporate data and look at it remotely without necessarily complying with the security policies and controls of the organisation.

Also, in all the sectors identified above, ensuring NIS in large companies and in SMEs is equally critical. Small and medium businesses have become the low-hanging fruit for cyber criminals and they need to be secure given that we are as strong as our weakest link.

On the other hand, micro companies are less critical for the overall continuity of the services given that incidents affecting them may not have a sufficiently wide reaching impact on society as those incidents affecting larger businesses.

4.1.5. What will happen if further measures are not adopted

4.1.5.1. Undermined consumer confidence in the internal market

The number of NIS incidents and their negative consequences will continue to increase and this will have a negative effect on the use of online public and private services, on consumers' trust in the on-line economy and in the integrity of the Internal Market.

The 2012 Eurobarometer on cyber-security found that 38% of users had concerns with the safety of on-line payments and have changed their behaviour because of concerns

³³ Summary report of the Expert Group on the security and resilience of communication networks and information systems for Smart Grids, July 2012, http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/expert_group_smart_grid/index_en.htm

with security issues: 18% are less likely to buy goods on-line and 15% are less likely to use on-line banking³⁴. The perceived lack of security on the Internet is thus having a negative effect on the functioning and development of the Internal Market. It is estimated that, by stimulating the development of the digital single market, Europe could gain 4% GDP by 2020³⁵. This GDP increase corresponds to a gain of almost €500 billion (€494 billion) or more than €1.000 for every citizen. In a time of economic downturn, this is not negligible.

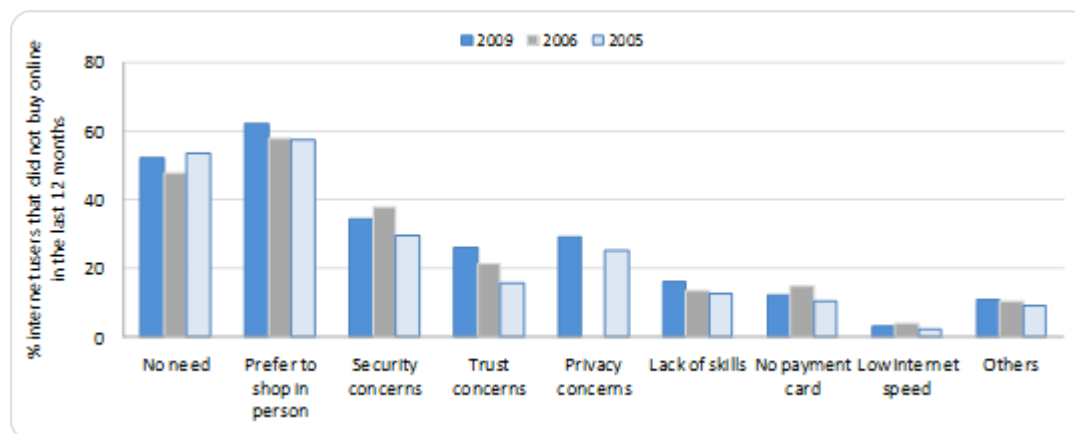


Figure 2: Reasons for Internet users not buying on-line in the EU countries, 2009.
Percentage of individuals with Internet access that did not buy on-line in the last 12 months

4.1.5.2. Insufficient business investments in NIS

Currently, businesses lack effective incentives to conduct serious risk management which involves the adoption of appropriate NIS measures (see also the relevant responses to the public consultation provided in Section 4.1.3). From an economic perspective security is an externality leading to a market failure³⁶, i.e. market players do not see the economic rationale to bear the full social costs of increasing the level of security but rather prioritise time-to-market or a low pricing for their end products. By leaving the decision on the level of security entirely to market players the societal benefits of a more secure digital environment would not be fully reached.

Often companies consider NIS a purely technical matter and do not address it as a key component of their business strategy, as a lynchpin for safeguarding their most precious assets notably intellectual property, financial information, and their reputation. Companies are often unaware of the risks faced until significant incidents occur and hence only adopt a reactive approach when circumstances require it. The same considerations apply to public administrations which do not yet see the importance of investing in NIS to ensure the continuity and reliability of the public services they provide more and more online.

³⁴ Idem Eurobarometer 390/2012

³⁵ Based on expected GDP for EU27 in 2010 of approximately €12 trillion. Copenhagen Economics, The Economic Impact of a European Digital Single Market, March 2010

³⁶ OECD 2008 'Economics of malware: Security decisions, incentives and externalities' <http://www.oecd.org/internet/interneteconomy/40722462.pdf>

According to Eurostat³⁷, by January 2012, 26 % of enterprises in the EU-27 had a formally defined ICT security policy with a plan for regular review; this share rose to over 50 % among those enterprises whose principal activity was information and communication activities. As shown in Figure 3, among the Member States, the highest shares of enterprises with a formally defined ICT security policy were recorded in Sweden and Denmark where more than two fifths of enterprises had such policies. The lowest shares of enterprises with a formally defined ICT security policy were on the other hand recorded in Bulgaria, Hungary, Romania, Poland and Estonia.

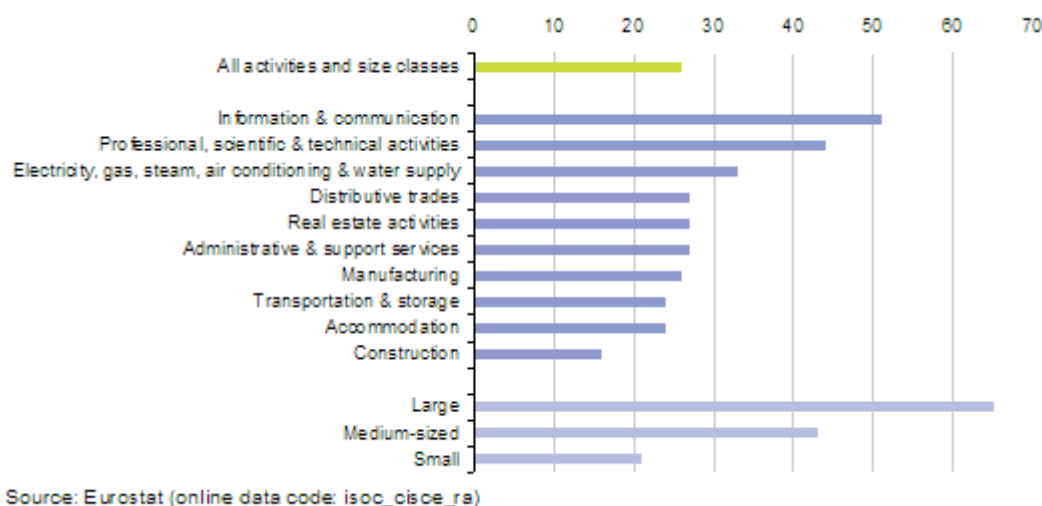


Figure 3 Enterprises having a formally defined ICT security policy with a plan of regular review, EU-27, January 2010 (% of enterprises) - Source: Eurostat ([isoc_cisce_ra](#))

Businesses are often unaware of the IT security risks faced and are overconfident about their actual level of protection; they perceive security costs as too high and see no business case for the return on investment on security³⁸. Indeed, businesses fail to see the potential savings induced by NIS investments. For example, the Ponemon 2011 Cost of Data Breach Studies for France, Germany and the UK showed that by appointing a Chief Information Security Officer (CISO) businesses could save up to half of the cost of a data breach.

The CSI 2007 Computer Crime and Security Survey found that the majority of companies (61%) allocate 5% or less of their overall IT budget to information security.

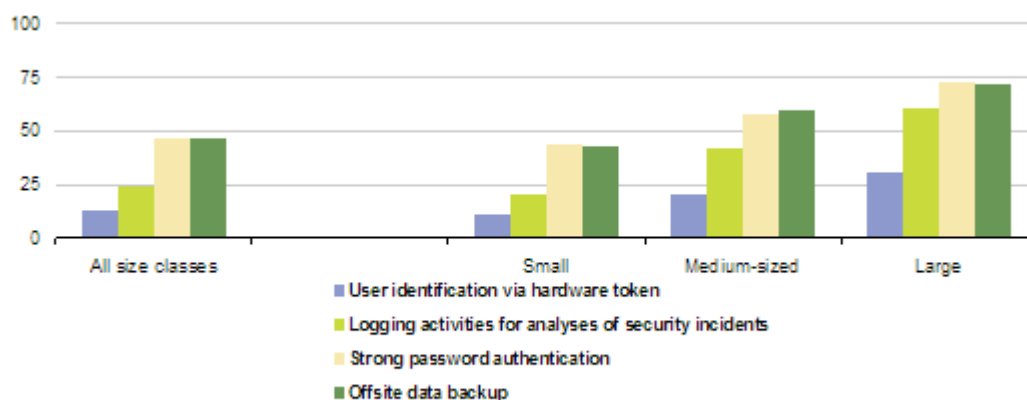
To counter the increasing number of web-based attacks, only 20% of business uses a secure protocol for the reception of orders via Internet³⁹.

As shown in Figure 4, small and medium-sized companies in the EU adopt less NIS measures than large companies.

³⁷ http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/ICT_security_in_enterprises

³⁸ The European Network and Information Security Market, IDC EMEA, 2009

³⁹ Eurostat, Community Survey on ICT usage in businesses, 2008



Source: Eurostat (online data code: isoc_cisce_fp)

Figure 4: Enterprises using internal security facilities or procedures, EU-27, January 2010 (% of enterprises) - Source: Eurostat ([isoc_cisce_fp](#))

4.1.5.3. Lack of credibility in the international scene

Without further actions at EU level, the Member States will act individually and will cooperate largely on a bilateral, multilateral or regional level. This would reduce the credibility of the EU at the international level, which would lead to the decay of existing cooperation arrangements, i.e. the EU-US Working Group on Cyber-security and Cybercrime⁴⁰ and would hinder discussions with other international partners. This will represent a lost opportunity to coordinate activities at global level and to achieve higher efficiency in addressing the problems.

Furthermore, higher credibility in NIS could boost economic potential and support as such the Internal Market.

4.2. Problem drivers: What is the reason behind the problem?

The problem of insufficient level of protection against network and information security incidents, risks and threats across the EU undermining the proper functioning of the Internal market stems from a range of factors.

4.2.1. Uneven level of capabilities across the EU⁴¹

Member States have very different levels of capabilities. This situation hinders the creation of trust among peers in the Member States which is an important prerequisite for cooperation and information sharing. While research⁴² suggests that certain Member States have now reached a high level of spending on NIS, some others have not.

⁴⁰ EU-US Summit 2010, Final statement, <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/597>

⁴¹ The information on the state of capabilities provided in this Section is based on the results of the stocktaking exercise carried out by Vice-President Neelie Kroes via two letters sent to Ministries in charge in the Member States respectively in 2011 and in 2012. Not all the Member States have participated to this stocktaking exercise however, the outcomes provide quite a clear overview of NIS capabilities across the EU.

⁴² Measuring the cost of cybercrime, June 2012, R. Anderson et al. http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

According to a market study⁴³, Member States can be divided into four groups on the basis of the maturity of their NIS markets:

Group 1, the Champions: Denmark, Finland, the Netherlands, Sweden, the United Kingdom

Group 2, the Pillars: Austria, Belgium, Germany, Luxembourg, France, Ireland

These two clusters account representing together 69% of the EU GDP but 82% of total security spending. These clusters are characterized by high average security spending, a strong presence of high profile security business users, and greater adoption of advanced security solutions.

Group 3, the Runners Up include the Southern European countries: Cyprus, Greece, Italy, Malta, Portugal, and Spain and: Czech Republic, Hungary and Slovenia.

This cluster shows some delay with the advanced clusters but a good potential for growth. They represent 30% of the EU population, 26% of EU GDP but 16% of the total EU NIS revenues

Group 4, the Learners: Bulgaria, Estonia, Latvia, Lithuania, Poland, Romania, Slovakia,

This cluster includes the remaining Member States with the lowest level of NIS spending and maturity. It represents 5% of EU GDP, but only 2% of NIS revenues) and shows a low number of connected PCs, with very low average security spending per connected PC.

Moreover, important considerations can be made following the stocktaking exercise that VP Neelie Kroes conducted across the Member States. The table below summarises the information provided by the Member States to Vice-President Kroes on their national capabilities. According to the information received, only group 1 countries and a large majority of group 2 countries have a level of preparedness which corresponds to the targets pursued by the Commission since 2009 (CIIP Action plan and CIIP Communication of 2011).

Group of countries	N/G CERTs	CERTs EGC ⁴⁴ group	NIS Strategy	Contingency/Cooperation Plan
1 - DK, FI, NL, SE, UK	DK, FI, NL, SE, UK	DK, FI, NL, SE, UK	DK*, FI, NL, SE, UK	DK, FI, NL, SE, UK
2 - AT, BE, DE, FR, IE,	AT, BE, DE,	AT, DE, FR,	AT, DE, FR,	AT, DE, FR, LU

⁴³ IDC EMEA study on the European Network and Information Security Market, April 2009. http://ec.europa.eu/information_society/policy/nis/docs/others_pdf/smart2007005_D_7_1.pdf

⁴⁴ Informal European Government CERTs Group

LU	FR, IE*, LU		IE, LU	
3 - CY, GR, IT, MT, PT, ES, CZ, HU, SL	CY*, GR, IT, MT, PT*, ES, CZ, HU, SL	ES, HU	CY, EL, ES, CZ, HU	CY, EL
4 - BG, EE, LV, LT, PL, RO, SK	BG, EE, LV, LT, PL, RO, SK		EE, LV, LT, PL, RO, SK	EE, LV

* In the process of adoption

4.2.1.1. Preparedness

Public sector players dealing with NIS in the EU include a large variety of ministries, agencies and National Regulatory Authorities⁴⁵. The existence of a plethora of bodies, each with different competences and responsibilities, makes it difficult for the Member States to identify their counterparts with whom to cooperate in other Member States. Not all the Member States have an operational national/governmental **CERT** in place to handle NIS incidents and prevent them from happening by monitoring threats. This uneven level of preparedness hinders cooperation on a European scale.

The European Government CERTs (EGC) group, which performs operational tasks, comprises only 10 Member States, which are the top performers. As indicated in the group's website⁴⁶: "Its members effectively co-operate on matters of incident response by building upon a fundament of mutual trust and understanding due to similarities in constituencies and problem sets".

Only some Member States have to date adopted national **cyber security strategies**.

4.2.1.2. Response

Not all Member States have in place a **cyber-incident contingency/cooperation plan**, providing protocols for communications and coordinated action in crisis situations, and not all the Member States have carried out or regularly carry out **cyber incident exercises**, which are major tools to put in place and test response capabilities.

All the Member States, supported by ENISA, have participated in the first pan-European cyber-incident exercise in 2010 (Cyber Europe 2010⁴⁷). According to the evaluation report of the exercise, the communication protocols differ from one Member State to another and there is hence a need for harmonisation of the existing communication processes, which also need to be made more secure⁴⁸.

⁴⁵ For overview see ENISA Who-is-Who Directory on network and information security <http://www.enisa.europa.eu/publications/who-is-who-directory-2011>. See also Annex 4 to this Staff Working Paper.

⁴⁶ See <http://www.egc-group.org/>

⁴⁷ <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1459>

⁴⁸ <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/ce2010/ce2010report>

In any serious crisis situation affecting networks and information systems, an appropriate response is vital and time critical. When threats or incidents have potential or actual cross border-nature, they need to be handled by the Member States in a coordinated and timely manner.

4.2.2. Insufficient sharing of information on incidents, risks and threats

Most security breaches go unreported and unnoticed mainly due to the reluctance of companies to share this information because of fear of reputational damages or liability. Often, people responsible for NIS share related information only with small groups they trust rather than going through official channels.

The insufficient sharing of information on threats and risks results in sub-optimal preparedness; the insufficient sharing of information on incidents results in sub-optimal response. The unavailability of reliable data and information on NIS threats and incidents makes it difficult for governments to conduct evidence-based policy making and to respond to incidents affecting governments' networks timely.

The lack of NIS data and information does not allow conducting appropriate analysis and compiling statistics that could be used to raise awareness of the rising threats and to plan appropriate measures to tackle them.

There is currently also no framework for trusted information sharing on security threats, risks and incidents amongst the Member States and between the private and the public sector. The UK stressed that mandatory reporting of security breaches may be a disincentive for those governments and businesses that are highly advanced in terms of NIS and that already pursue voluntary and cooperative arrangements. The UK would also favour a sector-specific approach to NIS given that risks and impact of incidents may differ from one sector to the other.

38% of respondents (both business and consumers) to the public consultation considered that effective sharing of information on threats and incidents would be best achieved by a requirement to report significant NIS security breaches to the national competent authority while 37% considered that it would be best achieved by stronger public-private cooperation mechanisms.

5. EFFECTIVENESS OF EXISTING MEASURES

5.1. There are loopholes in the existing regulatory framework

The only sector where companies are currently required under EU law to take NIS risk management steps and to report serious NIS incidents is the electronic communications sector⁴⁹.

The regulatory framework for electronic communications⁵⁰ requires providers of public electronic communications networks and services to appropriately manage the risks

⁴⁹ Respondents to the public consultation stressed that the financial industry is already required to manage NIS risks under certain national laws, e.g. in the UK, Netherlands and Germany. This would be accompanied by an obligation to report incidents to the national central bank or to the supervisory authorities. It may also be expected that those requirements will be further aligned as part of the plans to establish a European Banking Union

posed to the security of their networks and services to prevent and minimise the impact of security incidents on users and interconnected networks. It requires providers to notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services. These provisions had to be transposed at national level by 25 May 2011.

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.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data⁵¹ requires controllers of personal data to implement appropriate technical and organisational measures to protect personal data. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks presented by the processing and the nature of the personal data to be protected. In 2012, the Commission proposed a major reform of the EU legal framework on the protection of personal data⁵². Article 30 of the proposed General Data Protection Regulation⁵³ requires the data controller and the data processor to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation. The controller and the processor shall, following an evaluation of the risks, take security measures to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.

All players who are data controllers (e.g. a bank or a hospital) are hence already obliged to put in place security measures that are proportionate to the risks faced. On the other hand, data controllers would only be required to notify only those security breaches compromising personal data. A NIS breach affecting the provision of the service without compromising personal data (e.g. an ICT outage of a power company which results in a blackout) does not have to be notified.

The co-legislators are currently discussing the Commission proposal for a Directive on attacks against information systems⁵⁴. The proposed Directive focuses on penalising the exploitation of cybercrime tools. This proposal covers only the criminalization of specific

⁵⁰ Directive 2002/21 a common regulatory framework for electronic communications networks and services (Framework Directive), Article 13 a) and b) as introduced by Directive 2009/140/EC http://ec.europa.eu/information_society/policy/ecomm/doc/140framework.pdf

⁵¹ See <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT>

⁵² See http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

⁵³ COM(2012) 11

⁵⁴ COM(2010) 517, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF>

conducts, but does not address the prevention of NIS risks and incidents, the response to NIS incidents and the mitigation of their impact.

Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection⁵⁵ covers the energy and transport sectors. According to the Directive, the Member States had to go through a process of identifying potential European Critical Infrastructures (ECIs), with the help of the Commission if needed. The Directive also requires operators of identified European Critical Infrastructures to put in place security plans. 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. To date, only few European Critical Infrastructures have been identified as such by the Member States. The vast majority of the energy and transport players (e.g. airports, ports, electricity generators and gas distributors) are not covered.

In sum, the current rules do not require businesses other than telecommunication companies to adopt security measures and report NIS incidents, which do not affect personal data. The Diginotar case referred above illustrates the limits of this approach. Another striking example is the BlackBerry outage in 2011, which caused interruptions in basic communications services such as e-mail and SMS but did not have to be reported since the company is not a telecommunications operator and the incident did not compromise personal data.

Annexes 9 and 9 present the outcome of two specific benchmarking exercises that directly relate to how different aspects of the problem drivers have been dealt with in other sectors.

More precisely, Annex 8 provides an overview of current (regulatory) incentives for risk assessment and NIS in a number of sectors that strongly depend on NIS for the supply of their services. It is concluded that, in general, such incentives are insufficient in sectors other than the telecoms sector.

Annex 9 identifies and analyses a number of EU Early warning and incident handling networks in sectors other than NIS. These networks are used to share confidential information at EU level. Annex 8 provides useful insights on how such networks have been set up in the absence of mechanisms for effective cooperation at EU level.

5.2. The limits of a voluntary approach

The voluntary approach followed so far has resulted in an uneven level of preparedness and limited cooperation, as highlighted above. As a result the effectiveness of NIS capabilities varies considerably across the EU; cooperation takes place only amongst Member States who are well prepared, the others being left out or choosing themselves not to be involved.

The European Forum for Member States (EFMS) facilitates policy discussions and exchange of best practices between Member States. **The limited remit of EFMS means that the Member States do not share information on incidents, risks and threats**

⁵⁵ See <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF>

within the EFMS 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 provides **support and advice** to the Commission and the Member States with a view to improving the overall level of NIS in the EU. ENISA **has, however, no operational powers and, for example, cannot intervene to fix NIS problems.** The external evaluation⁵⁶ of ENISA in 2007 concluded that the value added of ENISA is its ability to provide an independent platform at the EU level for stakeholders and experts to discuss and compare problems and solutions regarding NIS and that the consensual view is that ENISA should be a well-established single European voice for security but that it should not be given more powers or an operational role. In addition, it must be borne in mind that there is no guarantee that the mandate of the Agency will be actually renewed after 2013.

The European Public-Private Partnership for Resilience (EP3R) is a platform which facilitates the exchange of best practices among the Member States and ICT companies. **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.

It can be reasonably assumed that without providing further directions to existing voluntary mechanisms, and specifically to the EFMS and the EP3R, the interest and the added-value in participating will decrease and this might lead to the possible dissolution of these mechanisms over time.

5.3. Approach in other regions of the world

Other regions of the world have adopted initiatives to address issues corresponding to the main problem drivers identified in this impact assessment.

In order to raise the level of security of critical information infrastructures, the US established in 1998 the National Infrastructure Protection Center (NIPC).

The National Cyber-security and Communications Integration Center (NCCIC) is an umbrella organisation set up in 2009 to coordinate national initiatives to address threats and incidents, including the US-CERT, National Coordinating Center for Telecommunications (NCC), the National Cyber-security Center (NCSC), and DHS Office of Intelligence and private sector partners from several ISACs.

Along with setting up dedicated capabilities of this kind, the US launched a series of Information Sharing and Analysis Centers (ISACs) for critical sectors⁵⁷ (including electricity, finance, health, maritime, ICT, nuclear, water), with the aim to ensure information sharing on threats and vulnerabilities between public and private sectors. The Industrial Control System Information Sharing and Analysis Center (ICS-ISAC) is the

⁵⁶ http://ec.europa.eu/dgs/information_society/evaluation/studies/s2006_enisa/docs/final_report.pdf

⁵⁷ See <http://www.isaccouncil.org/>

Private/Public center for knowledge sharing regarding Industrial Control System⁵⁸ (ICS) cybersecurity.

The lesson learnt from these experiences is that their effectiveness depends on the fact that the private sector shares information with the government and vice versa.

The US approach has inspired countries such as the UK, the Netherlands and Australia in setting up NIS capabilities. Although the US was first to establish a CERT already in 1988, the first government CERTs were established in the late 90's/early 2000's in UK, France, Germany, Netherlands and others and several of these came together to form the European Government CERTs group (EGC).

Regarding the reporting of security breaches, under US law companies are required to report security breaches for critical infrastructures does exist (Data Security and Breach Notification Act of 2012).

As a recent development, the Division of Corporation Finance of the US Securities and Exchange Commission released in 2011 guidance regarding public companies' disclosure obligations relating to cybersecurity risks and cyber incidents⁵⁹, due to concerns for the cyber-security risks faced by financial institutions. This shows that the US is now adopting an approach to cyber-security which covers key sectors where protection is essential, such as finance.

In Canada, "Industry Canada" is the lead agency for the Communications and Information Technology Sector and is responsible for CIP and emergency management. It has established the sector network – the Canadian Telecommunications Cyber Protection Working Group (CTCP) – to promote industry-to-industry, government-to-industry and industry-to-government co-operation in protecting Canadian networks. Industry Canada and CTCP have also established the Canadian Network for Security Information Exchange (CNSIE) to promote collaboration between a larger community of cyber security stakeholders such as the telecommunications, financial, energy, and vendor communities and government departments.

Regarding operational cooperation, the Organisation of American States has attempted to establish a 'hemispheric contact network' of CERTs but as yet the initiative has not flourished.

In the Asia-Pacific region, APCERT (Asia Pacific Computer Emergency Response Team) is a group of 30+ CERTs, mostly government CERTs. Membership is voluntary.

Japan's CERT capabilities were set up in 1996. JPCERT/CC coordinates with network service providers, security vendors, government agencies, as well as the industry associations and is acting as "CERT of CERTs" in the Japanese community. JPCERT/CC helped to set up APCERT. Also relevant is the Japanese Information-technology Security

⁵⁸ ICS are typically used in industries such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods.) Source: US Department of Commerce, <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>

⁵⁹ <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic4.htm>

Center (ISEC) established in 1997 as the public information sharing center for promoting information security in Japan, and the recently created Cyber Security Information Sharing Partnership (J-CSIP) providing a platform among critical infrastructures manufacturers.

In Australia the "Trusted Information Sharing Network (TISN)" is a forum in which the owners and operators of critical infrastructures work together, share information on threats and vulnerabilities and develop strategies and solutions to mitigate risk. It comprises seven critical infrastructure Sector Groups and two Expert Advisory Groups, Communities of Interest (CoI) and a Critical Infrastructure Advisory Council (CIAC).

Stakeholders mentioned the Australian Internet Security Initiative (AISI) as a cost-effective black-listing of IP addresses that are apparently compromised by malware and to dispatch that information to relevant ISPs and their customers.

5.4. Need of EU intervention, subsidiarity and proportionality

5.4.1. The EU right to act – Legal basis

The Union is empowered to adopt measures with the aim of establishing or ensuring the functioning of the internal market, in accordance with the relevant provisions of the Treaties (Article 26 Treaty on the Functioning of the European Union - TFEU).

In particular, Article 114 TFEU (former Article 95 EC) allows for the adoption of "measures for the *approximation of the provisions laid down by law, regulation or administrative action in Member States* which have as their object the establishment and functioning of the internal market" (emphasis added). Following the entry into force of the Lisbon treaty, the internal market is among the areas of "shared competence" between the Union and the Member States.

The ECJ held in Case C-66/04 that *"by the expression 'measures for the approximation' in Article 95 EC the authors of the Treaty intended to confer on the Community legislature a discretion, depending on the general context and the specific circumstances of the matter to be harmonised, as regards the harmonisation technique most appropriate for achieving the desired result, in particular in fields which are characterised by complex technical features."* (Paragraph 45).

Furthermore, in the international roaming case C-58/08, the ECJ held that:

"32. (...) the Community legislature may have recourse to (art. 114 TFEU) in particular where there are differences between national rules which are such as to obstruct the fundamental freedoms and thus have a direct effect on the functioning of the internal market (...) or to cause significant distortions of competition (...).

33. Recourse to that provision is also possible if the aim is to prevent the emergence of such obstacles to trade resulting from the divergent development of national laws. However, the emergence of such obstacles must be likely and the measure in question must be designed to prevent them (...)."

Several EU legislative acts based on Article 114 TFEU are related to NIS, showing that the EU legislator has already recognised the need to harmonise NIS rules to ensure the development of the internal market.

This was, in particular, the case for the ENISA regulation,⁶⁰ whose the Internal market legal basis was endorsed by the Court of Justice. The Court recognised⁶¹ that [it] *"was an appropriate means of preventing the emergence of disparities likely to create obstacles to the smooth functioning of the internal market in the area"*⁶²; and *"the smooth functioning of the internal market risks being undermined by a heterogeneous application of the technical requirements"*⁶³.

Regulation 460/2004/EC, establishing ENISA, states in Recital 3 that "the technical complexity of networks and information systems, the variety of products and services that are

⁶⁰ Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (OJ L 077, 13/03/2004, P 1-11).

⁶¹ ECJ 02.05.2006, C-217/04, United Kingdom of Great Britain and Northern Ireland v. European Parliament and Council of the European Union

⁶² Point 62.

⁶³ Point 63.

interconnected, and the huge number of private and public actors that bear their own responsibility risk undermining the smooth functioning of the internal market".

The 2010 Commission's proposal aimed at modernising and strengthening ENISA⁶⁴, currently under legislative procedure, is coherently based on Article 114 TFEU. As remarked in the Impact Assessment⁶⁵ accompanying the recent proposal for Regulation on ENISA "Uneven national policies and practices are a clear disruption of the internal market, due to the clear negative externalities resulting from NIS (inadequate policies impacting markets in other Member States), but also due to the positive externalities of good NIS practices (good practices in one Member State positively impact NIS as a whole, thus creating a clear societal good)".

The disparities resulting from uneven situations across the Member States in terms of capabilities, planning and level of protection, constitute at the same time a barrier to the internal market and justify EU action in cases with cross-border relevance, where coordination at the level of planning and at the level of response, including assistance, are needed.

Furthermore, information asymmetry and lack of transparency in the NIS market risk undermining the supply by market operators and manufacturers of networks, services and products as well as the trust of the users, which is one of the key drivers of the internal market.

Last, but not least, well-functioning networks and systems are essential for the functioning of our economy. Disruptions are increasing in frequency and magnitude undermining achievement of the digital agenda, which would have direct negative consequences for growth and jobs.

5.4.2. Subsidiarity test

Regulatory obligations are required to create a level playing field and close some legislative loopholes. A purely voluntarily approach has resulted in cooperation taking place only amongst a minority of Member States with a high level of capabilities. 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.

European intervention in the area of NIS is justified by the subsidiarity principle, due to the:

Cross-border nature of the problem

Given the cross-border nature of NIS threats and problems, a complete non-intervention at EU level would lead to a situation where each Member State is left to only guard its own backyard, with disregard of the interdependence between existing network and information systems. An appropriate degree of coordination among the Member States, on the other hand, would ensure that NIS risks can be well managed in the cross-border context in which they also arise, and therefore respects the subsidiarity principle.

⁶⁴ Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) of 30 September 2010, COM(2010) 521.

⁶⁵ SEC(2010) 1126

According to a recent study⁶⁶, differences in security regulations represent a (barrier to operating in multiple countries and to achieving global economies of scale. These differences lead to replication costs (up to 27 times) for pan-European operators. Harmonisation could lead to some economies of scale, but these differences are more or less inherent to the level of discretion enjoyed by the individual Member States regarding security and privacy.

Harmonising the implementation of regulation aimed at security and consumer protection is seen as an 'avoidable barrier'.

Effectiveness of the actions

Action at EU level would improve the effectiveness (and thus add value) to existing national policies, where they exist, or would facilitate their development.

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. European citizens are increasingly entrusting their data to complex information systems, either out of choice or out of necessity, without necessarily being able to correctly assess the related data protection risks. When incidents occur, they will therefore not necessarily be able to take suitable steps, nor is it certain that the Member States would be able to effectively address incidents with cross-border dimension in the absence of EU-wide NIS coordination. For this reason too, further policy action at the EU level seems to be widely justified.

5.4.3. Proportionality of the approach

The measures in the preferred option do not go beyond what is needed to achieve the objectives and do not impose disproportionate costs, as will be illustrated below.

The costs (see Section 8.2) that according to the preferred option would have to be incurred by those Member States lagging behind to put in place the necessary capabilities are not significant; for the others the costs will be negligible.

The costs for ensuring systematic cooperation amongst Member States according to the preferred option would be small when compared to the economic and societal losses and damages which may be caused by NIS incidents.

As to the private sector, should security requirements be set at EU level, they would apply only to some sectors for which the public consultation (see Section 4.1.4) underlined the importance of ensuring the security of network and information systems and markets and in which a serious NIS incident would have a direct and real-time effect on the EU economy and society. In any event, as indicated below, the measures proposed to ensure a basic level of protection would be proportionate to risks faced and hence reasonable and generally corresponding to the interest of the entities involved in ensuring continuity and quality of their services.

Moreover, many of these companies, as data controllers (e.g. banks and social networks) are already required by the current data protection rules to secure the protection of the personal

66

http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/cost_non_europe/im_e_com.pdf

data they control. For these companies the additional costs of the security requirements are likely to be marginal.

6. OBJECTIVES

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

6.1. Overview of general, specific and operational objectives

Specific objectives	Operational objectives
To put in place a minimum common level of NIS in the MS and thus increase the overall level of preparedness and response.	<ul style="list-style-type: none"> – To ensure that all Member States are adequately equipped at national level both in terms of technical and organisational capabilities to prevent, detect, mitigate and respond to NIS risks, threats and incidents. – To ensure that all Member States develop and update national cyber security strategies and national cyber incident contingency/cooperation plans.
To improve cooperation on NIS at EU level with a view to counter cross border incidents and threats effectively.	<ul style="list-style-type: none"> – To ensure that national competent authorities share NIS information and best practices regularly. – To make sure that such bodies can exchange information cross-border in a reliable and confidential manner.
To create a culture of risk management and improve the sharing of information between the private and public sectors.	<ul style="list-style-type: none"> – To make sure that key private sector players and public administrations engage in assessment of the risks and risk management practices. – To ensure that NIS breaches with a significant impact are reported to the national competent authorities.

6.2. Intervention logic

The intervention logic, linking the main problem and the drivers behind this problem to the specific objectives is illustrated in the next figure:

7. POLICY OPTIONS

The Policy options that have been considered in this Impact Assessment are: Business as usual, Regulatory approach and Mixed approach.

7.1. Discarded Option

The possible Option consisting of ceasing all EU activities on NIS has been discarded.

The Option would imply to stop pursuing the actions under the CIIP action plan and dismantling EFMS and EP3R.

All efforts undertaken in the area of NIS would be left entirely in the hands of the Member States and cooperation would remain limited to a small number of countries, with no virtually mechanisms in place for increasing trust among all of them.

The existing gap between the highly advanced and the less-advanced Member States would likely increase and so would the internal market failures associated to the divergences in the capabilities across the Member States. Such outcomes would not be consistent with DAE "digital single market" and Europe 2020 "smart and sustainable economy" objectives nor would it be efficient or effective for the Member States to tackle NIS cross-border problems on their own.

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

Under this Option the Commission, with the assistance of ENISA, would continue with its voluntary approach. With a view to put in place a minimum common level of NIS in the Member States and thus increase the overall level of preparedness and response, the Commission would continue issuing Communications addressing the Member States. Member States would be encouraged to set up well-functioning CERTs and to adopt a national cyber incident contingency/cooperation plan and a national cyber security strategy.

In order to improve cooperation on NIS at EU level, the Commission would recommend to the Member States to establish a network of CERTs across Europe and to adopt a European cyber incident contingency/cooperation plan. The Commission could also dedicate specific funds for building up one or more secure communication network across the EU.

The remit of the EFMS could be expanded to include discussions on the take-up of NIS best practises (e.g. how to best manage risks) by public administrations.

The Commission would also continue to stimulate the creation a culture of risk management and improve the sharing of information between the private and public sector by using platforms such as the EP3R.

Under this Option, ENISA would continue offering its support and expertise to the Member States and to the private sector, for example by issuing technical guidelines and recommendations on NIS capabilities and cooperation.

7.2. Option 2 – Regulatory approach

Under this Option, in order to reach a minimum common level of NIS across the EU and thus increase the overall level of preparedness and response, the Commission would propose to require all the Member States to:

- Set up a well-functioning national/governmental CERT, responsible for handling security incidents and risks according to a well-defined process and complying with essential requirements in terms of mandate and service provided. CERTs would need to have adequate staff and financial resources to carry out their tasks effectively.
- Appoint a national competent authority for NIS which would have a coordination role for NIS and act as a focal point for cross-border cooperation. The authority should be given appropriate technical, financial and human resources and be tasked with the elaboration of the national cyber security strategy (see below). The Member States may decide to have one single body acting both as a CERT and as a competent authority. The CERT would act under the supervision of the competent authority.
- Adopt a national contingency/cooperation plan defining protocols for communication and cooperation among relevant players at national level in case of NIS incidents of a certain scale.
- Adopt a national cyber-security strategy that would outline the strategic objectives and announce the concrete policy actions that each Member State intends to undertake to pursue a high level of NIS.

The establishment of such a common and comparable level of **capabilities** would be a precondition to enable cooperation across the EU.

In order to improve cooperation on NIS at EU level, the Commission would propose to mandate the national competent authorities to form a **network**, together with the Commission, to cooperate against EU level. ENISA would support the competent authorities in their cooperation by providing its expertise and advice.

Within the network the competent authorities would exchange information on serious threats and incidents and would cooperate via coordinated response to counter cross-border threats and incidents. This would occur in organised fashion according to the **European NIS contingency/cooperation plan** that the Commission would adopt following consultation with the Member States via Comitology.

The competent authorities would also ensure timely and regular publication on a common website of non- confidential information on on-going significant threats and incidents and on the coordinated responses adopted.

To build capacity and knowledge in the Member States, the competent authorities would within the network exchange best practices assist each other in building NIS capacities, organise regular peer reviews and pan-European NIS exercises.

The exchange of sensitive and confidential information between the competent authorities would take place through an infrastructure ensuring security and confidentiality.

The Member States would be able to access this secure infrastructure following a decision of the Commission to be taken by means of delegated acts and following assessment that the minimum NIS capabilities at national level described above are in place. The transposition/implementation period would allow the necessary delays for the Member States to comply with the requirements on national NIS capabilities.

Under this Option the Commission would also propose to impose NIS risk management and reporting requirements on public administrations (e.g. central ministries, local authorities, land registries) and key private players thus creating a comprehensive framework to stimulate the creation of a culture of risk management and improve the sharing of information between the private and public sectors. More specifically, the Commission would propose that operators in specific critical sectors, i.e. banking, energy (electricity and natural gas), transport, health, enablers of key Internet services and the public administration, be required to assess the risks they face and to adopt appropriate and proportionate measures to dimension the actual risks.

A detailed list of the entities that would be covered is provided at the end of this Section. An estimation of the actual number of those operators is provided along with the cost assessment in Annex 3. **Micro companies** (i.e. companies with less than 10 employees⁶⁷) would in any case **not be in the scope** of these obligations.

This requirement mirrors the one set out in Article 13a&b of the Framework Directive for electronic communications and would hence contribute to ensure a level playing field.

In order to give an indication of what this requirement may entail in practice, the ENISA guidelines on the security measures in Article 13a of the Framework Directive⁶⁸ can be taken as a sample. The activities that could fall under this requirement are:

- **Regular risk analysis** of specific assets for example information, software, physical assets, services and people. A number of standard methodologies exist for performing risk assessments, such as for example the ISO 27005 standard.
- **Governance and risk management** including establishing and maintaining an appropriate security policy; a governance and risk management framework to identify and address risks; an appropriate structure of security roles and responsibilities.
- **Human resources security**, i.e. adopting security measures to enhance the security of personnel such as employees, contractors and third-party users. This may include background checks; ensuring that personnel have sufficient knowledge and follows regular trainings; a process for handling security breaches committed by employees.
- **Security of systems and facilities**, that may include establishing and maintaining physical and environmental security of facilities; security of supplies and supporting facilities such as electric power, fuel or cooling; appropriate (logical) access controls

⁶⁷ Micro, small and medium enterprises are defined based on the criteria set out in [EU recommendation 2003/361](#)

⁶⁸ <https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/technical-guideline-for-minimum-security-measures-v1.0>

for access to network and information systems; appropriate security of network and information systems.

- **Operation management**, i.e. security of operation and management of network and information systems. This may include establishing and maintaining operational procedures and responsibilities and asset management procedures in order to verify asset availability and status.
- **Incident management**, i.e. establishing and maintaining standards and procedures for managing incidents. This may include establishing capabilities for detecting incidents and forwarding them to the appropriate departments within an appropriate time frame; processes for incident response and escalation; incident reporting and communication plans.
- **Business continuity management**, i.e. monitoring, testing and auditing of network and information systems, facilities and security measures, for example including policies for testing network and information systems.

Moreover, the entities indicated above would be required to report incidents with a significant impact on the services provided⁶⁹. This would also be in line with Article 13a&b of the Framework Directive.

These entities would have to report to the national competent authorities those incidents seriously compromising the operation of 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.

For example, an incident affecting an e-commerce platform and preventing the conclusion of on-line transactions over several hours would have to be reported. Likewise, a maintenance incident of an information system of a power plant, which results in stopping the distribution of electricity to a small city during several hours, would also have to be reported. National competent authorities would be empowered to request information, order security audits, issue instructions and carry out investigations on the players covered.

44.4% of respondents to the public consultation expressed the view that a requirement to notify and report incidents to NIS authorities would be needed to make private companies and public administrations systematically report about cyber security incidents.

57.4% of respondents to the public consultation expressed the view that support from NIS authorities to respond to incidents would be needed to the same purpose.

The reporting of breaches would be tightly linked to the cooperation among the competent authorities at EU level, given that the information fed to them would have to be shared with other competent authorities via the network when it has an actual or potential cross-border

⁶⁹ In their reply to the public consultation, Finland and GSMA underlined that a reporting obligation would require the competent authorities to have the ability to collect, combine, assess the criticality of notifications and distribute situational awareness on NIS incidents to relevant entities.

dimension. Also, competent authorities would have to prepare annually a summary report on the notifications received that would have to be provided to the Network.

Under this Option, ENISA would continue offering its support and technical expertise to the Member States and to the private sector, for example by issuing technical recommendations and guidelines on capabilities, on EU-level cooperation, on risk management and on the reporting of NIS incidents.

Entities that would be covered by risk management and NIS incidents reporting obligations are (more detailed indications are provided in Annex 3):

- **Energy** (electricity market and gas market):
 - Main electricity generating companies (i.e. those dealing with at least 5% of the country's electricity or gas)
 - Electricity retailers for final consumers
 - Entities bringing natural gas into the country
 - Retailers selling natural gas to final customers

The estimated total number of businesses affected in this sector would be approximately 4000.

- **Transport**
 - Air carriers (Freight and passenger air transport)
 - Maritime carriers (sea and coastal passenger water transport companies⁷⁰ and the number of sea and coastal freight water transport companies⁷¹)
 - Railways (infrastructure managers⁷², integrated companies⁷³ and railway transport operators⁷⁴)

⁷⁰ NACE Rev2 Code 50.1

⁷¹ NACE Rev2 Code 50.2

⁷² 'Infrastructure managers' are defined as 'Any enterprise or transport operator responsible in particular for establishing and maintaining railway infrastructure, as well as for operating the control and safety systems'.

⁷³ 'Integrated companies' are defined as: '*Railway transport operator also being an infrastructure manager*'. Railway transport operators include all public or private transport operators which provide services for the transport of goods and/or passengers by rail. Included are all transport operators that dispose of/provide traction. Excluded are railway transport operators which operate entirely or mainly within industrial and similar installations, including harbours, and railways transport operators which mainly provide local tourist services, such as preserved historical steam railways. Sometimes the term "railway undertaking" is used.

⁷⁴ Any public or private transport operator which provides services for the transport of goods and/or passengers by rail. Included are all transport operators that dispose of/provide traction. Excluded are railway transport operators which operate entirely or mainly within industrial and similar installations, including harbours, and railways transport operators which mainly provide local tourist services, such as preserved historical steam railways. Sometimes the term "railway undertaking" is used.

- Airports (EU airports with more than 15.000 passenger unit movements per year)
- Ports
- Traffic management control operators
- Auxiliary logistics services (a) warehousing and storage⁷⁵, b) cargo handling⁷⁶ and c) other transportation support activities⁷⁷)

The estimated total number of businesses affected in this sector would be approximately 14600.

- **Banking:** credit institutions⁷⁸ and stock exchanges

The estimated total number of businesses affected in this sector would be approximately 7706 for credit institutions and 25-30 for stock exchanges.

- **Health sector:** Hospitals including private clinics

The estimated total number of businesses affected in this sector would be approximately 15 000.

- **Enablers of Internet services**

These would include e-commerce platforms, social networks, search engines, cloud providers (Table 8 in Annex 2 provides a thorough indication of relevant players that would be in the scope). Software editors and providers would be excluded. The estimated total number of businesses affected in this sector would be approximately 1400.

- **Public administrations**⁷⁹, including local administrations

⁷⁵ NACE Rev2 Code 52.1: operation of storage and warehouse facilities for all kinds of goods: operation of grain silos, general merchandise warehouses, refrigerated warehouses, storage tanks etc.

⁷⁶ NACE Rev2 Code 52.24: loading and unloading of goods or passengers' luggage irrespective of the mode of transport used for transportation – stevedoring - loading and unloading of freight railway cars

⁷⁷ NACE Rev2 Code 52.29 forwarding of freight, arranging or organising of transport operations by rail, road, sea or air, organisation of group and individual consignments (including pickup and delivery of goods and grouping of consignments), issue and procurement of transport documents and waybills, activities of customs agents, activities of sea-freight forwarders and air-cargo agents, brokerage for ship and aircraft space, goods-handling operations, e.g. temporary crating for the sole purpose of protecting the goods during transit, uncrating, sampling, weighing of goods

⁷⁸ Credit institutions are defined by the EBC as '*commercial banks, savings banks, post office banks, credit unions, etc.*' (see <http://www.ecb.int/press/pr/date/2011/html/pr110114.en.html>)

⁷⁹ General government refers to all four sub-sectors of government (see 'Manual on Government Deficit and Debt, Methodologies and Working Papers, ISSN 1977-0375 - Implementation of ESA95' ; URL: http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-RA-09-017/EN/KS-RA-09-017-EN.PDF):

These are:

- *central government:* this includes all administrative departments of the State and other central agencies whose competence extends normally over the whole economic territory, except for the administration of social security funds;

It should be noted that this represent just an overall indication of the number of businesses that would be in the scope. Annex 3 provides a detail analysis of the process that led to these results.

The importance of ensuring NIS in these sectors has already been highlighted in Section 4.1.4 which also provides the views of the respondents to the public consultation on the importance to set NIS requirements for those who operate in these domains⁸⁰.

The same players should engage in NIS risk management and report NIS incidents with a significant impact to national competent authorities.

Only those players operating critical infrastructure and providing vital services relying on ICT significantly would be subject to these obligations. As explained in section 4.1.4 given their dependency on network and information systems, these players are particularly vulnerable to NIS incidents. These sectors are also critical for the economy and society and a serious NIS incident affecting them may produce significant negative side costs and often impair the functioning of the internal market. In many of these sectors a significant "network effect" can be observed, i.e. energy transmission or key online services are by definition provided over a network, the energy grid on the first case and the Internet in the latter. For these reasons the spill-over effects of an incident may be more difficult to contain.

It can be reasonably presumed that most of the players indicated above are, as data controllers, already required under the data protection regulatory framework to implement appropriate technical and organizational security measures to protect the personal data they handle. The following players are also data controllers:

- Energy distributors;
- Air, maritime, railway carriers;
- Credit institutions;
- Hospitals and private clinics;
- E-commerce platforms, social networks, booking engines; payment systems; operators of cloud computing platforms (in many cases)

-
- *state government* : this consists of separate institutional units exercising some of the functions of government at a level below that of central government and above that of the governmental institutional units existing at local level, except for the administration of social security funds;
 - *local government* : this includes those types of public administration whose competence extends to only a local part of the economic territory, apart from local agencies of social security funds;
 - *social security funds* : this includes all central, state and local institutional units whose principal activity is to provide social benefits and which fulfil each of the following two criteria: (1) by law or by regulation certain groups of the population are obliged to participate in the scheme or to pay contributions; (2) general government is responsible for the management of the institution in respect of the settlement or approval of the contributions and benefits independently from its role as supervisory body or employer.

⁸⁰ In the public consultation, some stakeholders expressed the view that sectoral regulation in some cases already empowers the regulatory bodies to address security issues. In their views the Commission needs to be careful to avoid unnecessary duplication or contradictions between its proposals and existing mechanisms.

- Public administrations

The table below (Figure 5) shows the extent to which existing obligations address NIS issues and what gaps would be filled by the preferred option.

	Covered by existing EU legislation	Not covered by existing EU legislation
Measures to ensure a high level of NIS	Data controllers across all sectors to adopt technical and organizational measures to protect personal data (Article 17, Directive 95/46/EC)	Technical and organisational measures to secure network and information systems beyond the purpose of protecting personal data across all sectors
	Providers of electronic communications networks and services to do NIS risk assessment and risk management (Article 13a&b, Directive 2002/21/EC)	
	Put in place security plans in European Critical Infrastructure in the energy and transport sector (around 20 infrastructure identified so far) (Directive 2008/114/EC)	
Measures to cooperate at EU level	Where appropriate, the national regulatory authority concerned shall inform the national regulatory authorities in other Member States (Article 13a, Directive 2002/21/EC)	Cooperation at EU level among authorities dealing with NIS or among sector-specific authorities sharing information on NIS risks and incidents
	Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the supervisory body concerned shall inform supervisory bodies in other Member States and ENISA (Article 15, Proposal for Regulation on e-identification and trust services)	
Measures to report NIS incidents	Notification of personal data breaches by data controllers across sectors to the supervisory authority and in specific cases to the data subject (Article 31 and 32, Proposal for Regulation on data protection Article 31 and 32)	Notification of security breaches which do not involve breaches of personal data across sectors
	Notification of personal data breaches by electronic communications providers to the competent national authority and in specific cases to the individual or subscriber (Article 4(3) of e-Privacy Directive 2002/58/EC)	
	Electronic communications operators to notify to the competent authorities breaches of security or loss of integrity with a significant impact on the operation of electronic communications networks	

	and services (Article 13a, Directive 2002/21/EC)	
	Trusted service providers to notify to the competent national body breaches of security of loss of integrity with a significant impact on the trust service provided and the personal data maintained therein (Article 15, Proposal for Regulation on e-identification and trust services)	

Figure 5: Table on existing regulatory gaps

7.3. Option 3 - Mixed approach

Under this Option, the Commission would combine voluntary initiatives based on the goodwill of the Member States, aimed at setting up or strengthening Member State NIS capabilities and at establishing mechanisms for EU-level cooperation, with regulatory requirements for key private players and public administrations on the adoption of NIS risk management measures and the notification of NIS incidents with a significant impact.

With a view to reach a minimum common level of NIS across the EU and thus increase the overall level of preparedness and response, the Commission would encourage the Member States, via Communications or Recommendations, to build **national capabilities** and particularly CERTs, to appoint a national competent authorities for NIS, to adopt national cyber incident contingency/cooperation plans and to adopt a national cyber security strategy.

In order to improve cooperation on NIS at EU level with a view to counter cross border incidents and threats effectively, the Commission would recommend to the Member States to establish a **network of CERTs** across Europe and to adopt a European cyber incident contingency/cooperation plan.

The remit of information sharing platforms such as **EFMS** could be further extended to include in the public policy exchanges taking place therein also public authorities from critical sectors such as banking, energy, transport or health.

These soft measures would be accompanied by regulatory requirements aimed at closing existing regulatory loopholes and create a level playing field across the EU.

In a view to stimulate the creation a culture of risk management and improve the sharing of information between the private and public sector, the Commission would propose to legally require public administrations and key private players in specific sectors (banking, energy - electricity and natural gas -, transport, health, postal services, Internet services and public administrations, see Option 2) to carry out risk management by assessing the risks they face and adopting measures appropriate to meet those risks.

In addition, public administrations and key private players will have to report to national competent authorities those incidents seriously compromising the operation of 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.

These regulatory requirements under Option 3 would hence be identical to those imposed under Option 2 both regarding the targeted entities and for the substance of the obligations.

The remit of EP3R could be further extended to include operators from additional critical sectors such as banking, energy, transport or health and continue to be a platform for the exchange of best practices between the public and the private sector.

Under this Option, ENISA would provide support and technical expertise to the Commission, the Member States and the private sector, for example by issuing technical guidelines and the recommendations on capabilities and EU-level cooperation, as well as on the take-up of risk management practises and on reporting security breaches.

This Option could have also been designed in other ways. In particular, it could have combined a regulatory approach for the Member States NIS capabilities and EU cooperation and a voluntary approach for the adoption of NIS risk management and for the reporting of NIS incidents by key private entities and public administrations.

The reason why this alternative combination was not considered is that a voluntary approach to risk management and incident reporting does not work for the reasons given in the Problem statement (i.e. insufficient business investments on security and lack of incentive to share information on NIS risks and incidents despite the worrying threat landscape).

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’)

The level of security

Despite the existing policy initiatives, it is unlikely that all the Member States would reach comparable levels of national capabilities and preparedness.

The mechanisms for cooperation and coordination at EU level would remain voluntary. In the absence of a minimum level of national capabilities in all the Member States, there would be no guarantee that cooperation involving all of them would take place. Lack of a framework and an infrastructure for sharing trusted information, based on common confidentiality requirements would also hinder such exchanges at EU level. Cooperation would continue within closed circles of Member States trusting one another. This would increase the gap between the high-performing and less-performing Member States.

The high-performing Member States have the ability to help businesses on their territories in detecting and responding to security incidents and this fosters cooperation between the public and private sector. In less-performing Member States market players' incentive to cooperate with the public sector will continue to be limited.

Only electronic communication providers would continue to be bound to adopt risk management practices and report breaches of security with a significant impact, on the basis of Article 13(a) of the Framework Directive. All other relevant market operators and public administrations would have no incentive to do so, other than purely commercial ones for

business. A level playing field would not be achieved and regulatory loopholes would continue to exist.

The lack of a comparable level of security and of cooperation across the Member States may also hinder international cooperation since it would be more difficult to present a common European position on NIS to foreign partners. Instead, non-European NIS stakeholders would have to liaise with the Member States (or just with some of them) on a bilateral basis, with the risk of adoption of different approaches. This would constitute a significant weakness in a domain where international cooperation is essential.

Economic impacts

The impact would depend on the extent to which the Member States would follow the Commission's recommendations. Given the voluntary nature of this approach, the pace of development would vary significantly across the EU. The insufficient level of security in the less developed Member States would undermine their competitiveness and growth by discouraging foreign companies from investing and doing business in these countries.

Given the interdependency of European networks and systems the negative impact of incidents, risks and threats on the EU economy as a whole (and not only in the less-prepared Member States) would increase overtime. Incidents related to NIS would become more and more visible to every business and consumers. This would seriously undermine the confidence in the digital environment and hinder the completion of the Internal Market.

Without improving the overall security framework in the EU we will not be able to reverse the trend of increasing security incidents and minimise their impact. Therefore, this option will come at a cost, which, as indicated in specific examples in the problem statement, is potentially very high.

Social impacts

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

The interests of citizens would be compromised when data are stolen, leaked, abused or corrupted due to a NIS incident, especially as no effective protection would be granted when data do not qualify as personal data.

As more and more critical sectors depend on network and information systems (including health care systems, financial services and significant portions of the public sector), incidents compromising their resilience would undermine the availability of the services provided by these critical sector sand this would cause significant societal harm.

Finally, with no harmonisation of NIS requirements within the Internal Market, employment in the information security industry will be hampered as it may be economically advantageous for European companies to tolerate occasional NIS incidents rather than investing in security, including via hiring and training competent personnel. Employment levels would hence under this Option remain suboptimal.

8.2. Option 2 – Regulatory approach

The level of security

Under this Option, the protection of EU consumers, business and Governments against NIS incidents, threats and risks would improve considerably.

The obligations placed on Member States would ensure that all of them are adequately equipped, both in terms of technical and organisational capabilities and preparedness. A common minimum set of requirements would contribute to the creation of a climate of mutual trust, which is a precondition for any effective cooperation at European level.

Secure and effective cooperation at European level would allow coherent and coordinated prevention and response to cross-border NIS incidents, risks and threats.

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 obligation for public administrations and key private players to report NIS incidents with a significant impact would enhance the ability to respond to incidents and would foster transparency. The availability of key data and information on NIS would also empower governments to carry out targeted analysis and compile statistics and hence to use reliable information on NIS to set the most adequate priorities in this domain.

The regulatory option, by enhancing the level of security, would enable the EU to demonstrate leadership in the area of NIS and become a more authoritative and effective player in international fora and in talks with its main international partners. By doing this, the EU will be better positioned to export its values and interests, thus also improving the protection of European citizens, businesses and administrations against threats originating outside the EU.

Economic impact

As a result of the increased level of security across the EU security problems would be more swiftly remedied and their impact diminished. The associated financial losses would also be reduced.

These benefits would be felt evenly across the EU, as potential divergences in national policies would be removed thus enabling a level playing field and supporting the development of the Internal Market.

This would improve business and consumers' confidence in the digital world and the Internet and so create new opportunities for business and the digital economy. Users will feel more secure on-line and this will improve their trust in the Internet to the benefit of the Internal Market.

In particular, the promotion of a risk management approach and a security culture would be beneficial to business and public administrations. Carrying out risk assessment would enable and incentivise them to efficiently allocate resources to manage NIS risks and would hence increase the value of the organisation to the public. Also, as businesses in the same sector would be required to implement similar security measures across the EU, businesses would compete on an equal footing.

Organisations would be better equipped to handle incidents and attacks, resulting in enhanced availability, reliability and quality of their services. This would raise the level of trust and satisfaction of those who use those services, increase profits and foster the development of the market. This is particularly important in markets requiring a high level of security for example the one for eHealth applications and the emerging cloud computing market.

The promotion of an enhanced risk management culture would also stimulate demand for secure ICT products and solutions. This would create new markets and opportunities in the EU and capitalise on the European research investments by improving prospects for their commercial exploitation.

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).

These crucial services would become more attractive due to their improved reliability and availability. This can highly empower citizens in rural or remote regions with limited access to offline services.

Finally, this Option is very likely to boost employment of NIS personnel in the EU due to the requirements to conduct NIS risk assessments and adopt appropriate security measures.

It is worth stressing that according to the "European Social Survey"⁸¹ the EU citizens find it important that governments ensure the safety of citizens against all threats. Moreover in 2010, compared to 2008, it was observed an increase in the percentage of citizens (67.2% against 63.2%) seeing a role for the government to ensure safety against all threats.

Impact on competitiveness

Overall impact on the EU economy

In general, it can be expected that an enhanced availability, reliability and quality of the services offered in critical sectors that rely heavily on network and information systems will benefit the competitiveness of the EU economy as a whole. For example, the availability of secure platforms for e-commerce and other web-based services could bring important economic benefits and allow a broad range of companies to bring new products and services to the market.

Sectoral competitiveness

Referring to the "Competitiveness proofing" toolkit⁸², a distinction can be made between⁸³:

- **Cost competitiveness:** the cost of doing business, which includes the costs of factors of production (labour, capital and energy);

⁸¹ <http://ess.nsd.uib.no/essmd>

⁸² Cf. 'Operational guidance for assessing impacts on sectoral competitiveness within the Commission IA system' (http://ec.europa.eu/governance/impact/key_docs/docs/sec_2012_0091_en.pdf)

⁸³ Cf. "Competitive proofing toolkit" – page 8.

- **Capacity to innovate:** the capacity of the business to produce more and/or better quality products and services that better meet customers' preferences;
- **International competitiveness:** the above two aspects could also be assessed in an international comparative perspective, so that the likely impact of the policy proposal on comparative advantages on the world markets is taken into account.

The impact on the competitiveness of the market of ICT security products and services can also be assessed.

Impact on competitiveness of sectors within the scope of the obligations

The impact in terms of **cost competitiveness** has been quantified⁸⁴ in Annex 2 on the compliance costs related to additional risk management measures and in Annex 3 on the administrative burden related to reporting significant NIS breaches. **It can be concluded that the additional costs in general remain limited since many measures have already been taken based on existing regulatory obligations.**

It may be expected that there will be an impact on the **capacity to innovate** of some of the entities within the scope. In some sectors, e.g. eCommerce platforms, booking engines, operators of cloud computing platforms, the new requirements could open opportunities to improve the features of current products or services (cf. '*capacity for product innovation*').

Finally, regarding **international competitiveness**, this Option would not differentiate between domestic and foreign business operating in the EU. *Competition in the internal market* would be improved by creating a level playing field via an enhanced harmonisation of NIS requirements, improved consistency of NIS risk management measures and coordinated response to incidents, enabled by a more systematic reporting of NIS incidents. For EU-based companies, the risk management measures (e.g. which are likely to result in compliance with international standards) could be considered as a competitive advantage when exporting products and services outside the EU (*competitive advantage in the external markets*).

Impact on competitiveness of ICT security products and service providers

A positive impact is finally also expected for the providers of ICT security products and services. First of all, demand is expected to increase. Furthermore, the development of specific security measures for the sectors within the scope, combined with a better harmonised approach at EU-level, will allow for innovative product development and economies of scale.

8.2.1. Cost estimations

In order to estimate the costs for the Member States to set up national NIS capabilities and participate in EU-level cooperation, it was made use of: 1) indications provided by the Member States during dedicated interviews 2) comparable initiatives and 3) opinions of NIS experts.

⁸⁴ Approach and data sources used are consistent with the best practice recommendations in the "Competitive proofing toolkit".

In order to estimate the magnitude of the impact on businesses and public administrations, use was made of comparable data provided by Eurostat, in Commission reports on regulated markets and statistics provided by sector-specific federations at European-level.

It must be borne in mind that reliable data on actual investments on NIS is difficult to find, given that companies are generally reluctant to disclose it given its confidential nature. Statistics on NIS expenditure of businesses are similarly scarce. It is difficult to assess how much is spent on NIS since it does not generally represent a separate budget line. Indications provided by Gartner⁸⁵ were used.

- (a) Costs for the Member States associated with building-up NIS capabilities and cooperation at EU level

The costs for NIS capabilities and cooperation would vary across the Member States, according to the respective current level of preparedness.

For the three Member States that have not yet established **national/governmental CERTs** (Cyprus, Ireland and Poland) the estimated cost of putting in place the related infrastructure and services based on interviews carried out with CERTs that are already operational would be **approximately 2.5 million EUR per CERT**.

As regards **NIS competent authorities**, it is likely that Member States would choose to designate existing bodies as competent authorities and assign additional tasks to these bodies. The corresponding additional costs should be regarded in terms of Full-Time Equivalents (FTE). Those Member States which have a sufficiently staffed authority in place would incur no additional costs.

Assuming that an average of 6 FTE per Member State (based on consultations with several national NIS bodies) would be required to carry out the tasks of a competent authority (i.e. developing and implementing a **cyber-incident contingency/cooperation plan** and a **national cyber security strategy**) the average cost would be **360 000 EUR per Member State**. The total theoretical maximum cost would be **9.72 million EUR across the EU** and de facto lower, since a few Member States already have co-ordinating cyber security centres or bodies in place.

As regards **pan-European cyber-incident exercises**, the first Cyber Europe exercise coordinated by ENISA in 2010 created an operational cost of 150 000 EUR for ENISA, with future exercises being expected to cost around 300 000 EUR. A total of 150 experts from the Member States were involved in 2010. Assuming that each expert dedicated two fulltime months on average to the exercise, the exercise would have required the equivalent of 25 FTE or a total of 1.5 million EUR for all the Member States per pan-European exercise and 750 000 EUR for all the Member States per year, assuming that a pan-European exercise takes place every two years. This would mean a cost **per Member State of 55 555 EUR per exercise**.

The costs related to the cooperation among the competent authorities within the **network** would be limited to travel and subsistence expenses, only when travelling would be required. Assuming two participants per Member State and three meetings per year with an average

⁸⁵ <http://www.gartner.com/technology/home.jsp>

cost of 1000 EUR for travel and subsistence, the cost **per Member State** would stand at approximately **6000 EUR per year**.

The costs related to the common website where the competent authorities would timely and regularly publish non-confidential information on threats, incidents and response adopted would amount to a **setup cost of 5000 EUR** (estimating that it would take 25 days and 2/3 technician and 1/3 project manager to setup the website including meetings, specifications, visual design, implementation, going online). This would be an EU-average manpower cost⁸⁶. On a recurrent basis, the cost would be 200 EUR/month⁸⁷ and hence **2400 EUR/year** for the EU (this would cover among the others hosting and domain name).

The costs for carrying out tasks linked to this website, e.g. providing content and promoting the website, would be covered by the costs for the competent authorities that have been illustrated above.

The costs for establishing the **physical infrastructure** necessary for the sharing of information in the Network of competent authorities and CERTs would depend on whether the Member States would decide to use an existing infrastructure or to set up a dedicated one.

The cost of the physical infrastructure would depend on whether the Member States would choose to use and adapt an existing infrastructure (e.g. sTESTA⁸⁸) or to establish a new one. In the former case it has been estimated that the cost would be **about 1 million EUR** (based on the cost for the adaptation of the system that was developed by the JRC for the early warning and response system in public health) and can be borne by the EU budget, budget line 09.03.02 (to promote the interconnection and interoperability of national public services on-line as well as access to such networks - Chapter 09.03, Connecting Europe Facility – telecommunications networks) on condition that funds are available under the Connecting Europe Facility (CEF); alternatively, the related costs would have to be shared among the Member States. In the latter case (setting up of a new infrastructure) the related cost has been estimated to be **10 million EUR** per year for the EU as a whole (this is the cost currently incurred by the Commission in relation to sTESTA, which is provided by the French network operator Orange) and would have to be shared among the Member States.

(b) Compliance costs for public administrations and key private players

The additional NIS spending that would be required has been calculated as the difference between the target level of spending according to current best practices and the current actual spending in the various relevant sectors (taking into account the estimated annual natural increase in spending due to rising NIS threats).

The target level adjusted by the natural increase in spending is 6.61% of a company's total IT spending.

The total additional NIS compliance costs would hence be in the range from **1 to 2 billion EUR**.

⁸⁶ Assuming a cost of 150 EUR for a technician and of 300 EUR for a project manager.

⁸⁷ Considering that one man*day/month (2/3 technician, 1/3 project manager) should suffice

⁸⁸ <http://ec.europa.eu/idabc/en/document/2097.html>

This estimation takes into account that most of the entities affected are already supposed to be compliant with existing security requirements, namely the obligation for data controllers to take technical and organisational measures to secure personal data, including NIS measures. Thus, the present Option would primarily entail new efforts and costs for entities which do not qualify as data controllers.

The costs have been hence reduced by a certain factor to take into account existing spending on security.


Given that the magnitude of this reduction is hard to estimate with precision, different scenarios are taken into account, namely the numbers in bold in table 5 indicate the total additional costs when a 70% cut is applied (left column) and when a 40% cut is applied (right column), respectively.

	Range of additional ICT spending required, caused by NIS Regulation (Compliance cost of the NIS Regulation)					
	Per sector		Per company		in % of turnover	
	Mill EUR		EUR			
Energy	0,0	0,0	0	0	0,000%	0,000%
Transportation	118,0	236,0	8.084	16.168	0,032%	0,064%
Banking and financial services	170,0	340,0	21.975	43.951	0,023%	0,047%
Healthcare providers	67,4	134,7	4.501	9.003	0,023%	0,045%
ICT sector (excl. telecom)	4,4	8,9	3.238	6.476	0,015%	0,030%
TOTAL (excl. public sector)	359,8	719,6			in % of OPEX	
Public sector	577,4	1.154,8			0,026%	0,052%
TOTAL	937,2	1.874,5				

Table 5: Estimated additional spending for compliance with NIS risk management obligations

As regards SMEs⁸⁹, they are the back-bone of the European economy as they constitute more than 99% of all European businesses.

A considerable number of these companies are micro-enterprises, i.e. companies which employ less than 10 people. They have been excluded from the scope since they do not have the scale nor do they provide the services that would fall within the scope of the requirements. Also, NIS incidents affecting micro enterprises and a consequent discontinuity of the services offered by these companies may not have a sufficiently wide reaching impact on society as those incidents affecting business of larger size. For this reason, regulatory measures on these players would not be justified.

⁸⁹ Micro, small and medium enterprises are defined based on the following criteria (cf.: EU recommendation 2003/361 

Company category	Employees	Turnover	or	Balance sheet total
Medium-sized	< 250	≤ € 50 m		≤ € 43 m
Small	< 50	≤ € 10 m		≤ € 10 m
Micro	< 10	≤ € 2 m		≤ € 2 m

However, there are small (up to 50 employees) and medium enterprises (from 50 to 250 employees) to which the requirements would apply.

Starting from the total compliance costs for the private sector (see Table 5), which range from 360 to 720 million EUR, the compliance cost **per small and medium enterprise** would fall in the range of **2500 and 5000 EUR**. In carrying out the calculation, it has been assumed that small and medium enterprises account for 20% of the turnover of the private companies concerned by the regulation and represent 68% of all the companies affected or just over 28 000 enterprises.

Annex 3 provides a detailed indication of the entities involved, their turnover or operating expenditure, and the additional costs that would have to be borne.

Regarding costs that would have to be borne by SMEs, Annex 4 provides the SME-test.

- (c) Costs for public administrations and key private players associated with reporting NIS incidents with a significant impact

In order to value the costs for reporting serious NIS incidents, an estimation of the notifications that would be done over one year has been extrapolated from existing data on the implementation of Article 13a of the framework directive for electronic communications. On this basis, the number of NIS incidents notifications expected would amount to approximately 1700 per year. Assuming that one employee would have to devote 0.5 working day for the notification, and that the notification as such would have a negligible costs (e.g. it would be done via an e-mail) the **expected cost per breach notification would be 125 EUR**, leading to a **total cost for notifying breaches on an annual basis of 212 500 EUR at the EU level**.

Regarding possible investigations that can be initiated by the NIS competent authorities on the compliance with risk management and NIS incidents notification obligations, it is not possible at this stage to estimate if and how many investigations could be initiated. It can however be reasonably assumed that 10 to 20% of the NIS incidents notifications might be followed by an investigation, corresponding to an absolute value of 170 to 340 expected investigations per year.

Taking into account the standard salary cost, the maximum cost for the entity affected would be **maximum 25 000 EUR per investigation** or **4.25 million to 8.5 million EUR per year across the EU**.

The costs for the annual reporting on notifications that the competent authorities would have to prepare and deliver to the Network would already be included in the costs indicated above for the Member States to adequately staff and equip the competent authorities.

A detailed analysis of the process that led to these estimations is provided in Annex 4.

8.3. Option 3 – Mixed approach

The level of security

Under this Option, it is unlikely that all the Member States would reach comparable levels of national capabilities and preparedness via voluntary initiatives.

As a consequence, in the absence of a minimum level of national capabilities in all the Member States, there would be no guarantee that cooperation involving all of them would take place.

Given that also mechanisms for cooperation and coordination at EU level would remain voluntary, cooperation would continue within closed circles of Member States trusting one another. Lack of a framework and an infrastructure for sharing trusted information, based on common confidentiality requirements would also hinder exchanges at EU level. This would increase the gap between the high-performing and less-performing Member States.

On the other hand, the introduction of security requirements for public administrations and key private players would create a strong incentive for those players to manage and dimension security risks effectively. These mechanisms would however be ineffective in those Member States who would not follow the Commission recommendations on the setting up of NIS capabilities. For example, without a national competent authority being appointed, there would be no organisation or body to which NIS incidents could be reported.

Also, it is unlikely that public administrations would be able to carry out appropriate NIS risk management in those Member States where NIS capabilities would not be in place at the level of the central government (e.g. CERT or national competent authority).

Overall, under this Option the EU would miss an opportunity to increase the general level of NIS, as progress would still be patchy.

The lack of a comparable level of security and of cooperation across the Member States would harm the effectiveness of international cooperation as described in the assessment of Option 1. This would constitute a significant weakness in a domain where international cooperation is essential.

Under this Option, the EU as a whole would not demonstrate leadership in the area of NIS and not be well positioned to export its values and interests.

Economic impacts

Given the voluntary nature of this approach, 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 by discouraging foreign companies from investing and doing business in these countries. Also, the less performing Member States would be more exposed to the negative impact of incidents, risks and threats.

The public administrations and the private sector would adopt measures to remedy problems more swiftly and to dimension their impact. However, given the continuing weakness of certain Member States, the overall level of security in the EU would remain low and hence the impact of incidents, risks and threats on the EU economy would increase overtime.

Without securing the weakest link, incidents would become more and more visible to business and consumers. This would undermine the confidence in the digital environment and hinder the completion of the Internal Market.

The regulatory requirements on public administrations and key private players would however stimulate demand for secure ICT products and solutions. This would also create new markets

and opportunities in the EU and capitalise on the European research investments by improving prospects for their commercial exploitation.

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.

Although the NIS requirements for key private players and public administrations could generate the social benefits described in the assessment of Option 2 in terms of increased use of digital technologies, citizens' empowerment and boost of employment, the likely disparities in the Member States' approach to NIS would generally hinder such benefits.

Finally, this Option is very likely to promote employment of NIS specialised personnel in the EU due to the requirements to conduct NIS risk assessments and to adopt appropriate security measures in a number of sectors.

Costs

The costs for setting-up national NIS capabilities and for the cooperation at EU level will depend on the extent to which the Member States would conduct these activities on a voluntary basis.

The compliance costs for public administrations and market operators will be identical to those described above under Option 2.

9. COMPARING THE OPTIONS

9.1. Overall comparison of the assessment

The previous chapters presented a detailed assessment of the three selected policy options.

Given the urgency to enhance the level of protection against NIS incidents, threats and vulnerabilities as described above, and the need to implement the policy objectives that are proposed in this impact assessment to address the problem drivers, it must be concluded that Option 1 and 3 are not to be 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 cooperate 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. In particular, the obligations on Member States would ensure adequate preparedness at national level; the setting up of coordinated mechanisms at EU level would deliver EU-wide coherent and coordinated prevention and response; the establishment of common NIS requirements for public administrations and key private players would foster a strong culture of risk management and would curb information asymmetry in the market. 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.

Annex 13 specifies the extent to which each policy option contributes to the achievement of the objectives. The assessment of the impacts under each of the options was done by analysing the *magnitude* of the expected impact, as well as the *likelihood* that the impact will actually occur as a result of the proposed policy option. According to these criteria Policy Option 2 has scored the highest in achieving the objectives.

9.2. Overall cost-benefit analysis

The table below (Figure 6) provides an overview of the costs related to each of the 3 policy options. The Table shows that Option 2 would entail the highest costs as a consequence of the regulatory approach. Costs stemming from Option 3 would be slightly lower as the Member States' spending for NIS capabilities and for participating in EU cooperation will depend on the goodwill of each Member State. The table also shows benefits for each option, as explained in the assessment of the options presented in the previous Section.

	Option 1 Business as usual	Option 2 Regulatory approach	Option 3 Mixed approach
a) Costs related to setting-up national NIS capabilities and participation in EU cooperation			
<i>Setting up of national/governmental CERT</i>	Between 0 and 7.5 million EUR (Depending on the precise capabilities the MS without CERT would develop with no obligation to do so)	Approximately 2.5 million EUR per CERT per year (for the three MS not having a CERT yet (Cyprus, Ireland and Poland), 0 EUR for the MS already having a CERT in place)	Between 0 and 7.5 million EUR (Depending on the precise capabilities the MS without CERT would develop on a voluntary basis)
<i>Establishing Competent Authorities</i>	N/A	Maximum 9.72 million EUR (360 000 EUR per MS) per year (For the EU 27, this relates to on average six additional FTEs per MS to be added in an existing organisation)	Between 0 and 9.72 million EUR (Depending on the precise capabilities that would be developed on a voluntary basis)
<i>Set-up of common website for the publication of non confidential information on NIS threats</i>	N/A	5 kEUR (set-up cost for the website) 2.4 kEUR (yearly recurring cost for the website)	Between 0 and 5 kEUR (set-up cost) Between 0 and 2.4 kEUR (yearly recurring cost) (Depending on the intention of the MS to develop and maintain voluntarily a website of this kind)
<i>Cooperation of competent authorities within a network</i>	N/A	6 kEUR per MS per year (Only relevant cost relates to travelling and subsistence, assumption of 3 meetings per year and two participants per MS per meeting)	6 kEUR per MS per year (Depending on the degree of additional cooperation that would be put in place on a voluntary basis)
<i>Participating to pan-European exercises</i>	750 kEUR for all MS per exercise (or ± 28 kEUR per year per MS) (For the EU 27, this relates to the participation of 150 experts, involved during two months for an exercise every two years)	750 kEUR for all MS per exercise (or ± 55.5 kEUR per MS per exercise) (For the EU 27, this relates to the participation of 150 experts, involved during two months for an exercise every two years. It is also assumed that the increased cost of a future increase of the scope of the exercise would be compensated by an increased efficiency).	750 kEUR for all MS per exercise (or ± 28 kEUR per year per MS) (For the EU 27, this relates to the participation of 150 experts, involved during two months for an exercise every two years)
<i>Establishment of the physical infrastructure ensuring secure information exchange</i>	N/A	Around 1 million EUR for adapting sTESTA (borne by EU if funds are available under CEF or cost shared among the Member States) or 10 million EUR per year for a new dedicated network comparable to sTESTA (cost to be shared among the Member States)	N/A (It is assumed that the establishment of an EU wide physical infrastructure would not be realised on a voluntary basis)
b) Compliance costs for public administrations and key private players (related to NIS risk management measures)			
<i>Adoption of additional risk management measures</i>	N/A	1 to 2 billion EUR in total (per year for all sectors considered) 6.5 kEUR to 44 kEUR on average per company, depending on the sector 2.5 to 5 kEUR per SME within the scope of the Regulation	Idem Option 2
c) Administrative burden for public administrations and key private players (related to reporting NIS incidents with a significant impact)			
<i>Reporting on incidents with a significant impact</i>	N/A	125 EUR per breach notification Maximum 25 000 EUR per investigation	Idem Option 2
	Competitiveness and growth not ensured; risk of undermining citizens' interests and critical services; decreased online confidence of citizens; employment hampered; difficulties in presenting a common EU position internationally	Swift remediation of incidents and reduced related costs; enhanced trust in the digital economy and in the internal market; creation of market for security solutions; enhanced competitiveness; enhanced citizens' opportunities and employment; EU more authoritative internationally	Competitiveness and growth not ensured; overall risk that citizens' interests and critical services will be undermined and that online confidence will decrease; employment opportunities enhanced; creation of a market for security solutions

Figure 6: Comparative table of costs for the three Policy options

An overall cost-benefit analysis would require a quantification of the possible benefits of compulsory measures to ensure a high level of NIS across the EU. Some of these benefits can be directly linked to fact that NIS incidents would have no or little impact when NIS measures

are in place. Other benefits are more general and relate for example to the effects of increased confidence in the digital economy.

Assessing the magnitude of the possible benefits in this particular context is extremely difficult for a number of reasons and in particular given that:

- There is an incomplete view of the frequency and gravity of NIS incidents;
- There are general indications that the number, frequency and complexity of NIS incidents are on the rise. However, there is no information on the pace of this increase nor are there sufficient quantitative elements available on how the situation is today so to estimate the absolute magnitude of this increase;
- It is difficult to assess to what extent enhanced NIS would mitigate the negative impact of security incidents.

Some of the measures proposed (especially those on the reporting of NIS incidents) are meant, at least to some extent, to address this lack of data. Beside the positive effects on trust in the digital economy and the internal market, the main benefits of this option will stem from the likely contribution to decreasing the costs of security incidents, including malicious attacks. The following estimates indicate the scale of these actual or potential costs:

- According to the World Economic Forum, in the next ten years there is a 10% likelihood of a major Critical Information Infrastructure breakdown with potential economic damages of over \$250 billion.
- The global consumer cybercrime is estimated at **100 billion US \$ worldwide** (per year); there are moreover clear indications that cybercrime is starting to focus their efforts on the increasingly popular platforms such as social networks and mobile devices⁹⁰.
- The cost of cyber-crime in the UK, related to Intellectual Property (IP) theft and industrial espionage, was estimated by Detica⁹¹ at **21 billion £ per year**. The cost of cyber-crime for government was estimated at **2.2 billion £ per year** (total cost of tax and benefits fraud, local government and central government fraud, national health services (NHS) fraud and pension fraud). The study furthermore stresses that the full economic impact goes beyond the direct costs that were identified in the study.

10. MONITORING AND EVALUATION

This Section proposes measures to monitor and evaluate the impact of the preferred option, on the basis of the three specific objectives that such Option aims at achieving.

First of all, the Commission would periodically review the functioning of the legislation particularly on the basis of technological and market developments and would provide a report to the European Parliament and the Council every three years.

⁹⁰ See http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02

⁹¹ See 'The Cost of Cyber Crime' – a Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office.

The review process would also be supported by targeted studies, information received from the Member States, expert discussions, workshops, Eurobarometer statistics, etc.

The core indicators and tools in the table below provide a general framework for monitoring and evaluation.

Core indicators of progress towards meeting the objectives:

Specific objectives	Monitoring indicators	Tools
To put in place a minimum common level of NIS in the MS and thus increase the overall level of preparedness.	<ul style="list-style-type: none"> Number of Member States having appointed a NIS competent authority which is adequately staffed and equipped to carry out EU-level cooperation Number of Member States having established national/governmental CERTs which meet the pre-defined minimum baseline requirements Number of Member States having adopted a national cyber-security strategy Number of Member States having adopted a national Cyber incident contingency/cooperation plan 	<ul style="list-style-type: none"> Surveys of competent authorities Comparative implementation reports on national cyber security strategies, the role of competent authorities, functioning of CERTs and national cyber security contingency/co operation plans
To improve cooperation on NIS at EU level with a view to counter cross border incidents and threats effectively.	<ul style="list-style-type: none"> Number of competent authorities cooperating via the network Number of competent authorities participating in the secure information exchange Information exchange among the competent authorities on NIS incidents, risks and threats 	<ul style="list-style-type: none"> Surveys of competent authorities Progress report on the implementation of the European cyber incident contingency/co operation plan Assessment of the outcome of capacity

	<ul style="list-style-type: none"> • Implementation of the European cyber incident contingency/cooperation plan • Reduced divergence of Member States' approaches to NIS • Number of NIS cyber incident exercises at EU level • Number of conferences/meetings between Member States to define commonly agreed goals for NIS • Capacity building activities involving the Member States • EU-wide NIS practices • Collection of comparable data on NIS by the competent authorities • Regular and timely publication of non-confidential information on threats, incidents and response on a common website 	<p>building activities involving the Member States (e.g. based on country case studies)</p>
<p>To create a culture of risk management and improve the sharing of information between the private and public sectors.</p>	<ul style="list-style-type: none"> • Regular NIS risk assessment by public administrations and key private players • Level of investments in NIS by public administrations and key private players • Number of notifications of NIS incidents with a significant impact to the competent authorities (the sum of this number and the number of public administrations and companies which have 	<ul style="list-style-type: none"> • Survey of players within the scope of NIS requirements to assess the level of NIS investments and the best practices adopted to ensure NIS • Surveys of competent authorities to evaluate the

	<p>failed to notify security breaches should be decreasing over time)</p> <ul style="list-style-type: none"> • Governments' access to information and data on actual NIS incidents (on the basis of the notifications received) and possibility to carry out analysis and compile statistics and to set priorities on NIS accordingly 	<p>incidents notifications received (incl. e.g. case studies and peer reviews assessing in more detail the reporting obligations put in place in the Member States</p> <ul style="list-style-type: none"> • Comparative implementation report on the criteria applied for defining a significant breach
--	--	--

ANNEX 1: PUBLIC CONSULTATION ON NETWORK AND INFORMATION SECURITY ACROSS THE EU

SUMMARY OF ANSWERS RECEIVED

An online public consultation ran from 23 July to 15 October 2012.

The total number of respondents which submitted replies through the on-line tool was 169 and the breakdown of the related answers is reflected in the statistics provided below.

A further 10 organisations submitted written replies outside the on-line tool, bringing the total number of replies to the public consultation to 179; these 10 are not reflected in the statistics but their written contributions will be published online.

The total breakdown by type of respondent is the following: 88 individuals (of which 57 asked to remain anonymous); 11 public authorities (of which 5 asked to remain anonymous); 80 organisations or institutions such as businesses, research institutions and NGOs (of which 41 intend to remain anonymous).

Type of respondent	Not anonymous	Anonymous	Outside the on-line tool (not included in statistics)	Total
Individuals	31	57	-	88
Public authorities	4	5	2	11
Other organisations (businesses, research institutions, NGOs etc.)	31	41	8	80
Total anonymous/not anonymous	66	103		
Total replies through on-line tool [66+103]	169		Total replies incl. outside on-line tool [169+10]	179

The questions posed in the online public consultation focused on:

- **Scale of the problem and evidence on impact**, to assess whether the respondents had experienced significant incidents and what are in their opinion the most frequent causes of NIS incidents.

- **Improving NIS through an EU strategic approach**, to assess whether the respondents believe that there is sufficient awareness of threats and incidents in the EU, that governments do enough in this field and what incentives can be set to ensure reporting of incidents and to raise user awareness.
- **Improving NIS in the EU through risk management and reporting of incidents**, to assess whether the respondents conduct risk management; for which sectors of activity they believe it would be important to have NIS requirements; whether they would in principle agree with the introduction of regulatory requirements to manage NIS risks and what additional costs a requirement of this kind would entail for them. To assess also how effective information sharing could be achieved; to whom and at what level a requirement to report NIS incidents should be set; and what additional costs a reporting requirement would imply.

Regarding the **Scale of the problem and evidence on impact**, most of the respondents (56.8%) affirmed having experienced over the last year NIS incidents with a serious impact on their activities.

The respondents expressed the view that the most frequent cases of NIS incidents are third party/external failure (47.3%), malicious attacks (40.8%), software/hardware failure (36.1%) and human/technical errors (27.8%).

Regarding **Improving NIS through an EU strategic approach**, a very large majority (82.8%) of the respondents expressed the view that consumers are in general not aware of existing NIS risks. A comparable high majority (82.8%) of the respondents also affirmed that governments in the EU should do more to ensure a high level of NIS.

When asked what kind of incentives would be needed to make companies and public administrations systematically report about NIS incidents, a large number of respondents affirmed that those could entail support from NIS authorities to respond to incidents (57.4%), notification and report to NIS authorities (44.4%) and publicity of incidents and establishment of performance ranking (44.4%). Only 8.9% of the respondents affirmed that no incentives are needed in this regard.

Regarding the reporting of NIS incidents that may also constitute cybercrime to law enforcement, many respondents suggested that this objective could be achieved at EU level by establishing a legal requirement for NIS authorities, CERTs and affected users (39.6%) or only NIS authorities and CERTs (24.9%). On the other hand, 35.5% of the respondents said that nobody should be legally required to report to law enforcement incidents that may constitute cybercrime, but that everybody should be strongly encouraged to do so.

A very large majority of respondents (84%) affirmed that businesses, governments and consumers in the EU are not sufficiently aware of the behaviour to be adopted to minimise the impact of the NIS risks they face. The respondents suggest that the best ways to achieve this objective would be in particular to give guidance at EU level to enable consumers to differentiate good security products and services (30.2%), to define compulsory security standards for goods and services at EU level (30.2%) or to stimulate the development of industry-led standards (18.3%).

Regarding **Improving NIS in the EU through risk management and reporting of incidents**, 31% of the respondents affirmed that they do not have a process for managing risks in place and 54.2% of the respondents said that they do not have a budget dedicated to NIS. 30% of the respondents also affirmed that they did not have sufficient resources in place to counter and minimise the effects of NIS incidents that have affected them.

The large majority of respondents expressed the view that the adoption of NIS requirements would be important or very important in specific sectors in particular banking and finance (91.1%), energy (89.4%), transport (81.7%), health (89.4%), Internet services (89.1%) and public administrations (87.5%).

The majority of respondents would also in principle be favourable to the introduction of a regulatory requirement to manage NIS risks (66.3%) at EU level (84.8% of those respondents). 70.5% of those respondents also suggested that this requirements entail a general obligation to adopt state of the art measures proportionate to the risks identified.

Some of those respondents indicated that those who should be subject to these requirements are all business and consumers providing or using network and information systems (41.5%) whereas others (41.5%) said that only business providing or using network and information systems underpinning vital services for society (i.e. transport, energy, finance, health, Internet services of general interest, water) should be subject to this requirement.

The respondents stressed that a requirement to adopt NIS risk management according to the state of the art would entail for them no additional significant costs (43.6%) or no additional costs at all (19.8%). 36.5% of the respondents said that this would entail significant additional costs for them.

Regarding incentives for effective information sharing on threats and incidents, the respondents suggest to establish a requirement to report significant NIS breaches to the national competent authority (37.9%) or to establish stronger public-private cooperation mechanisms (37.3%).

The majority of the respondents (65%) expressed the view that if a requirement to report NIS security breaches to the national competent authority were introduced it should be set at EU level and affirmed that also public administrations should be subject to it (93.5%).

If this requirement were to be introduced at EU level, respondents mainly suggested that this should apply only to business providing or using network and information systems underpinning services which are vital for the functioning of the society (43.8%) or to all business and consumers providing or using network and information systems (34.9%).

The majority of the respondents (52.5%) also affirmed that a requirement to report security breaches would not cause significant additional costs for them and 19.8% said that it would not cause additional costs at all for them.

ANNEX 2: ACTION PLANS AND STRATEGIES ADOPTED SO FAR IN THE FIELD OF NIS IN THE EU

In its Communication "Network and Information Security: Proposal for A European Policy Approach" of 2001, the Commission outlined the increasing importance of NIS for our economies and societies⁹². As part of its response to security threats, the European Community decided in 2004 to establish the European Network and Information Security Agency (ENISA)⁹³ to ensure a high and effective level of NIS in the EU. The role of ENISA is to contribute to the development of a culture of NIS for the benefit of citizens, consumers, enterprises and public sector organisations in the European Union and to provide advice to the European Commission to this effect. A Commission proposal to update and extend ENISA's mandate is under discussion in the Council and European Parliament⁹⁴.

In 2006, a Strategy for a Secure Information Society⁹⁵ was adopted in response to the urgent need to coordinate efforts for building up trust and confidence of stakeholders in electronic communications and services. Already the 2006 Strategy ambitioned to further develop a dynamic, global strategy in Europe based on a culture of security and founded on dialogue, partnership and empowerment. The main elements of this strategy were endorsed in a Council Resolution⁹⁶.

The Commission adopted, also in 2006, its proposal for a "European Programme for Critical Infrastructure Protection (EPCIP)"⁹⁷ which sets forth the overall "umbrella" approach to the protection of critical infrastructures in the EU. One of the EPCIP implementation actions is Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection⁹⁸ that covers the energy and transport sectors.

The Safer Internet Programme⁹⁹ 2009-2013 was launched in 2008 and provides a strong foundation to promote safer use of the Internet and other communication technologies, particularly for children, and to fight against illegal content and harmful conduct online.

After an intensive process of consultation with all relevant stakeholders, the Commission adopted, on 30 March 2009, a Communication on Critical Information Infrastructure protection (CIIP)¹⁰⁰ focusing on the protection of Europe from cyber-attacks and cyber disruptions by enhancing preparedness, security and resilience. The Communication launched an action plan with five pillars of actions: preparedness and prevention; detection and response; mitigation and recovery; international cooperation; criteria for the ICT sector. The CIIP Action Plan put forward, for the ICT sector, the necessary sector-specific policies

⁹² COM(2001)298

⁹³ See Regulation (EC) No 460/2004 at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=-CELEX:32004R0460:EN:HTML>

⁹⁴ COM(2010)521 [e](#)

⁹⁵ COM(2006)251 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf

⁹⁶ 2007/068/01

⁹⁷ COM(2006)786 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf

⁹⁸ See <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF>

⁹⁹ Decision No 1351/2008/EC
http://ec.europa.eu/information_society/activities/sip/docs/prog_decision_2009/decision_en.pdf

¹⁰⁰ COM(2009)149 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF>

complementing the overall European Programme for Critical Infrastructure Protection (EPCIP).

The Action plan was endorsed in the Presidency Conclusions of the Ministerial conference on CIIP in Tallinn in 2009. These commitments were further advanced by the Council Resolution on "A collaborative European approach to network and information security"¹⁰¹ adopted on 18 December 2009.

The revised regulatory framework for electronic communications¹⁰² in force since November 2009 set new security provisions including on security breaches notifications (Art. 13a&b of the Framework Directive), that were to be transposed at national level by 25 May 2011.

Security and resilience issues are notably addressed under the Trust and Security chapter of the Digital Agenda for Europe¹⁰³, one of the flagship initiatives of the EU2020 Strategy. In particular, Key action 6 of the Digital Agenda for Europe calls for measures aimed at a reinforced and high level NIS policy.

The Digital Agenda for Europe is complementary to other initiatives such as the Stockholm Programme for Freedom, Security and Justice and the Internal Security Strategy in action (ISS)¹⁰⁴. The Stockholm Programme/Action Plan¹⁰⁵ and the ISS underline the Commission's commitment to building a digital environment where every European can fully express his or her economic and social potential.

More recently, the Commission second Communication on CIIP of March 2011 on "Achievements and next steps: towards global cyber-security"¹⁰⁶ took stock of the results achieved since the adoption of the CIIP action plan in 2009 and described the next priorities planned under each action both at EU and at the international level. Council Conclusions on CIIP were adopted on 27 May 2011¹⁰⁷. The 2011 CIIP Communication contains a number of actions in which the Commission calls upon the Member States to set up NIS capabilities and cross-border cooperation. Most of these actions should have been completed by 2012, but as highlighted in Section 4.2.1, they have not been yet implemented.

Discussions are also on going as regards the Commission proposal for a Directive on attacks against information systems¹⁰⁸ which aims at harmonising the criminalisation of specific conducts.

¹⁰¹ 2009/C 321/01

¹⁰² See http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf

¹⁰³ COM(2010)245, http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf

¹⁰⁴ COM(2010)673 lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF

¹⁰⁵ COM(2010)171 [http://eur-](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:EN:PDF)

¹⁰⁶ COM(2011)163 [http://eur-](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF)

¹⁰⁷ [http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede150611cccyberse](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede150611cccybersecuri/_sede150611cccybersecurity_en.pdf)

¹⁰⁸ COM(2010) 517, [http://eur-](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF)

Recently, the Commission adopted a Communication¹⁰⁹ on the establishment of a European Cybercrime Centre (EC3), which would be part of Europol and act as the focal point in the fight against cybercrime in the EU. EC3 is intended to pool European cybercrime expertise to support Member States in capacity building, provide support to Member States' cybercrime investigations and become the collective voice of European cybercrime investigators across law enforcement and the judiciary.

At the international level, since the 2010 EU-US Summit¹¹⁰, a joint EU-US Working Group on Cyber-security and Cybercrime has been established.

The EU is also active in relevant international multilateral fora, such as the Organisation for Economic Co-operation and Development (OECD), the United Nations General Assembly (UNGA), the International Telecommunication Union (ITU), the Organisation for Security and Co-operation in Europe (OSCE), the World Summit on the Information Society (WSIS) and the Internet Governance Forum (IGF). The EU also actively participates to the London process on cyberspace.

A revised CIP policy package is foreseen for adoption in the coming months. The objective is to review EPCIP, including Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection.

¹⁰⁹ COM(2012)140
[lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF)

¹¹⁰ http://europa.eu/rapid/press-release_MEMO-10-597_en.htm

[http://eur-](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF)

ANNEX 3: ASSESSMENT OF NIS RISK MANAGEMENT COMPLIANCE COSTS FOR PUBLIC ADMINISTRATIONS AND KEY PRIVATE PLAYERS

Introduction

Assumption taken regarding the scope of relevant costs

All public administrations and key private players would under Option 2 and 3 be required to conduct risk assessment and to put in place risk management measures proportionate to the risks faced.

As in the electronic communications sector, the threshold for significance could be defined in relation to the impact that the breach may have on the operation of networks or services. A very important aspect in this regard is the *perspective of the consumers or citizens* that could be affected, and this is something that will vary from sector to sector. For example, for hospitals, this threshold would not relate to the number of patients that could be affected (size of the hospital), but to the seriousness of a possible breakdown of the network and information systems for a single patient, e.g. in case a crucial medical system goes down during surgery. Taking into account this criterion and for each of the sectors presented below, an assessment is provided of the number of companies affected and the financial impact on them. Micro-companies would be excluded.

Methodology for the cost assessment

- STEP 1: Identification of relevant sectors (based on Scope of Options 2 and 3) incl. estimation of their revenues/turnover
- STEP 2: Identification of the cost related to ICT security spending that is currently not yet made ‘naturally’ by the organisations and which can be considered as ‘underinvestment’
- STEP 3: Assessment of the additional cost for risk management that could be caused by NIS risk management obligations .

STEP 1: Identification of relevant sectors and entities, incl. turnover

In the following, an estimation is made of the number of entities that are expected to be impacted by the risk assessment obligations, as well as of their turnover (so as to be able to make further calculations in the following steps). The exercise is done for each of the following sectors separately:

- **Energy market** (electricity market and gas market)
- **Transport sector** (operators of air transport, rail transport and maritime transport; incl. auxiliary logistic services)
- **Financial sector** (all credit institutions and stock exchanges)
- **Health sector** (hospitals)

- **Enablers of Internet services** (excl. telecom operators already within the scope of the Telecom Framework Directive)
- **Public administrations**

It should be noted that results presented below should be treated with caution, i.e. the goal is to obtain an overall idea of the **type and number of entities** and subsequently of the order of magnitude of the impact.

Energy market

The energy market can be further subdivided in the electricity and gas market. More precisely, the actors within the scope of the risk management requirements are:

- Electricity generating companies
- Electricity Transmission and Distribution System Operators (TSO and DSO)
- Entities bringing natural gas into the country
- Gas Transmission and Distribution System Operators (TSO and DSO)

Recent data on the number of these companies in the EU is not yet available in the Eurostat dissemination database, but can be found at:

http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Electricity_market_indicators

http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Natural_gas_market_indicators

Furthermore, the DG ENERGY ‘Report on progress in creating the Internal Gas and Electricity Market’ (2009-2010) also gives some indications of the number of Transmission System Operators (TSOs) and Distribution System Operators (DSOs): http://ec.europa.eu/energy/gas_electricity/legislation/doc/20100609_internal_market_report_2009_2010_annex.pdf.

As for the generating companies, only the ‘main’ companies (those dealing with at least 5% of the country’s electricity or gas) are considered to be particularly critical. Possible problems in energy supply by smaller generators due to NIS breaches will easily be tackled by other companies, thus not resulting in a significant impact. For retailers, the situation is different, as a breach in NIS for one company can have a direct significant impact on its customers, regardless of the size of the company. Therefore, all electricity and gas transmission and distribution operators are assumed to be relevant for inclusion. This leads to a **total number of businesses affected**, equal to **approximately 4000**:

	ELECTRICITY SECTOR			GAS SECTOR			
	Number of main electricity generating companies	Number of Transmission System Operators (TSO) - Electricity	Number of Distribution System Operators (DSO) - Electricity	Number of main entities bringing natural gas into the country	Number of Transmission System Operators (TSO) - Gas	Number of Distribution System Operators (DSO) - Gas	Total number of companies
	2010	2009	2009	2010	2009	2009	
Belgium	3	1	26	3	1	18	52
Bulgaria	5	1	129	1	1	28	165
Czech Republic	1	1	3	3	1	79	88
Denmark	2	1	84	2	1	3	93
Germany	4	4	866	7	18	695	1.594
Estonia	1	1	38	1	1	26	68
Ireland	6	1	1	6	1	1	16
Greece	1	1	1	3	1	3	10
Spain*	4	1	351	5	14	22	397
France	1	1	148	3	2	25	180
Italy	5	9	144	3	3	263	427
Cyprus	1	1	1	0	1		4
Latvia	1	1	11	1	1	1	16
Lithuania	5	1	2	4	1	6	19
Luxembourg	2	1	6	1	1	4	15
Hungary	3	1	6	6	1	10	27
Malta	1	0	1	0	1		3
Netherlands	5	1	8		1	10	25
Austria	4	3	129	4	7	20	167
Poland	5	1	20	1	1	6	34
Portugal	2	3	13	2	1	11	32
Romania	6	1	36	2	1	38	84
Slovenia	2	1	1	2	1	18	25
Slovakia	1	1	3	3	1	46	55
Finland	4	1	88	1	1	23	118
Sweden	5	1	170	2	2	5	185
United Kingdom	8	1	20	7	4	20	60
EU27	88	41	2.306	73	70	1.381	3.959

Table 1: Overview of number of affected businesses in the electricity and gas sector per MS

To estimate the revenues of these businesses, an extrapolation is made with the help of another data source, namely Eurostat structural business statistics. Whereas this source provides for information at the level of the much broader ‘electricity, gas and water supply sector’¹¹¹, it is useful to derive a unitary value for the average turnover of a company in the sector, which can then be extrapolated to the volumes presented above. More precisely, with the help of the Eurostat figures an average turnover per business is derived by dividing the total¹¹² sector turnover by the number of enterprises in the sector:

¹¹¹ See Eurostat, Structural business statistics, NACE_R1 Code E comprises ‘Electricity, gas and water supply’ and is the best proxy available for estimating the average turnover of electricity and gas companies.

¹¹² Only taking into account medium-sized and large enterprises, i.e. micro- and small enterprises do not intervene in the calculation as they are considered not relevant for inclusion in the scope (cf. the broad definition of the NACE_R1 code E comprising around 28.000 companies whereas only electricity and gas generating and retailing companies are targeted here).

<i>in mill EUR</i>	Companies with from 50 to 250 persons employed	Companies with 250 persons employed or more	Total (over 50 persons employed)
Turnover	137.308	544.205	681.513
Number of companies	2.120	960	3.080
Average turnover per company	65	567	221

Table 2: Estimation of average company turnover (based on NACE_R1 Code E)

This average turnover per business resulting from the Eurostat data is then combined with the total number of businesses as presented in the table above (i.e. 3959 companies), leading to a total turnover at the EU level of 876 billion EUR (visible in summary Table 11).

Transport sector

The relevant activities within the transport sector relate to those for which a significant NIS incident would have some kind of ‘network effect’ impacting other actors in the sector, resulting easily in a wide spread impact, incl. cross border, and thus impacting an important number of customers (citizens as well as businesses).

Based on this criterion, operators in the air, rail and maritime transport sector are considered to be key operators that would fall within the scope of the obligations (both infrastructure owners and operators/service providers over these infrastructures), and this for both passenger and freight transport. As for freight transport, next to the transport companies *stricto sensu*, also companies providing auxiliary logistics services (such as warehouse operating and cargo handling), irrespective of the mode of transport, should be included in this scope, as they are an equally vital part in the time-critical transport flow of goods. To define the number of companies active in each of these subsectors in the EU, the following sources were used:

Air transport:

- In terms of infrastructure, Eurostat provides for statistics on the number of main airports in the EU (with more than 15 000 passenger unit movements per year): http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=avia_if_arp&lang=en
- As for airlines, Eurostat also has information on the number of companies active in passenger air transport¹¹³ and freight air transport¹¹⁴, but for passenger air transport these figures do not only include commercial airlines, but also e.g. operators of scenic and sightseeing flights, thus resulting in a very high overall figure that is not representative for the EU market targeted. The Eurostat figures per Member State are therefore only taken into account for freight air transport, and for passenger air transport use is made of a general indication of the size of the market by DG TREN (see factsheet on the sector http://ec.europa.eu/transport/air/doc/03_2009_facts_figures.pdf), and the number of passenger air operators at the EU level that is provided by them is further distributed

¹¹³ NACE Rev2 Code 51.10

¹¹⁴ NACE Rev2 Code 51.21

over the individual Member States according to the distribution of freight air transport companies.

- Traffic control for air transport is usually not provided by the operator/owner of the infrastructure, so that these types of companies form a separate category for the air transport subsector. Information on the number of companies could not be found, but revenue data is reprised below.

Railway transport:

- Number of railway operators in the EU can be found in Eurostat (total of infrastructure managers¹¹⁵, integrated companies¹¹⁶ and railway transport operators¹¹⁷):
http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=rail_ec_ent&lang=en

Maritime transport:

- For the number of ‘operators’ on the market, Eurostat provides information on the number of sea and coastal passenger water transport companies¹¹⁸ and the number of sea and coastal freight water transport companies¹¹⁹ per Member State.
- As for the infrastructure, i.e. the ports, DG MOVE states there are about 1 200 ports in the EU¹²⁰, and by lack of readily available data per Member State, this total is distributed over the individual Member States according to the distribution of freight maritime transport companies (this does not influence results for the EU total, but has as a consequence that the data at Member State level should be treated with caution).

Auxiliary logistics services:

- The EU statistical system has a separate section on ‘warehousing and support activities for transportation’, of which a) warehousing and storage¹²¹, b) cargo

¹¹⁵ ‘Infrastructure managers’ are defined as ‘Any enterprise or transport operator responsible in particular for establishing and maintaining railway infrastructure, as well as for operating the control and safety systems’.

¹¹⁶ ‘Integrated companies’ are defined as: ‘*Railway transport operator also being an infrastructure manager*’. Railway transport operators include all public or private transport operators which provide services for the transport of goods and/or passengers by rail. Included are all transport operators that dispose of/provide traction. Excluded are railway transport operators which operate entirely or mainly within industrial and similar installations, including harbours, and railways transport operators which mainly provide local tourist services, such as preserved historical steam railways. Sometimes the term “railway undertaking” is used.

¹¹⁷ Any public or private transport operator which provides services for the transport of goods and/or passengers by rail. Included are all transport operators that dispose of/provide traction. Excluded are railway transport operators which operate entirely or mainly within industrial and similar installations, including harbours, and railways transport operators which mainly provide local tourist services, such as preserved historical steam railways. Sometimes the term “railway undertaking” is used.

¹¹⁸ NACE Rev2 Code 50.1

¹¹⁹ NACE Rev2 Code 50.2

¹²⁰ http://ec.europa.eu/transport/maritime/ports_en.htm

¹²¹ NACE Rev2 Code 52.1: operation of storage and warehouse facilities for all kinds of goods: operation of grain silos, general merchandise warehouses, refrigerated warehouses, storage tanks etc.

handling¹²² and c) other transportation support activities¹²³ seem most relevant, i.e. excluded are support activities to land, water and air transportation as they contain elements that are already reprised in the subsectors for specific modes of transport above (e.g. harbour operation), whereas others do not comply with the criteria for inclusion with respect to the proposed measures. It should be noted that for this subsector, the relevancy of companies for inclusion in the scope highly depends on the size of the company, i.e. only NIS incidents in large companies in this type of business are expected to be able to have a significant impact in terms of creating blockings or other problems in the network. Detailed data on the number of large companies for b) and c) are not available, but volumes can be estimated by taking into account the percentage of large companies in the overall subsector 'support activities for transportation'¹²⁴.

The scope of companies presented above, leads to **a total estimated number of businesses equal to ± 14 600** that are considered as relevant in the transport sector:

¹²² NACE Rev2 Code 52.24: loading and unloading of goods or passengers' luggage irrespective of the mode of transport used for transportation – stevedoring - loading and unloading of freight railway cars

¹²³ NACE Rev2 Code 52.29 forwarding of freight, arranging or organising of transport operations by rail, road, sea or air, organisation of group and individual consignments (including pickup and delivery of goods and grouping of consignments), issue and procurement of transport documents and waybills, activities of customs agents, activities of sea-freight forwarders and air-cargo agents, brokerage for ship and aircraft space, goods-handling operations, e.g. temporary crating for the sole purpose of protecting the goods during transit, uncrating, sampling, weighing of goods

¹²⁴ NACE Rev2 Code 52.2