



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

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

**concerning measures to ensure a high common level of network and information
security across the Union**

{SWD(2012) xxx}

{SWD(2012) xxx}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

The aim of the proposed Directive is to ensure a high common level of network and information security (NIS) across the EU. This will be achieved by requiring the Member States to increase their preparedness and improve their cooperation with each other, and by requiring operators of critical infrastructure and public administrations to adopt appropriate steps to manage security risks and report serious incidents to the national competent authorities.

This proposal is presented in the context of the joint Communication of the Commission and High Representative of the Union for Foreign Affairs and Security Policy on a European Cybersecurity Strategy. The objective of the Strategy is to ensure a secure and trustworthy digital environment, while promoting and protecting fundamental rights and other EU core values. This proposal is the main action of the Strategy. Further actions of the Strategy in this sphere focus on awareness-raising, the development of an internal market for cybersecurity products and services and fostering R&D investments. These actions will be complemented by those aimed at stepping up the fight against cybercrime and at building an international cybersecurity policy for the EU.

1.1. Reasons for and objectives of the proposal

NIS is increasingly important to our economy and society. However, information systems can always be affected by security incidents, such as human mistakes, natural events, technical failures or malicious attacks. These incidents are becoming bigger, more frequent, and more complex. The Commission's online public consultation on "Improving network and information security in the EU"¹ found that 57% of respondents had experienced NIS incidents over the previous year that had a serious impact on their activities. Lack of NIS can compromise the vital services depending on the integrity of network and information systems. As a consequence, it can stop businesses functioning, generate substantial financial losses for the EU economy and negatively affect societal welfare.

Moreover, as a borderless communication instrument, digital information systems and primarily the Internet, are interconnected across Member States and play an essential role in facilitating the cross-border movement of goods, services and people. Substantial disruption of these systems in one Member State can affect other Member States and the EU as a whole. The resilience and stability of network and information systems is therefore essential to the completion of the Digital Single Market and the smooth functioning of the Internal Market as a whole. The likelihood and the frequency of incidents and the inability to ensure efficient protection also undermine public trust and confidence in network and information services: for example, the 2012 Eurobarometer on Cybersecurity found that 38% of EU Internet users have concerns with the safety of on-line payments and have changed their behaviour because of concerns with security issues: 18% are less likely to buy goods on-line and 15% are less likely to use on-line banking².

The current situation in the EU, as it results from the purely voluntary approach followed so far, does not provide sufficient protection against NIS incidents and risks across the EU. The existing NIS capabilities and mechanisms are simply insufficient to keep pace with the fast-

¹ The online public consultation on "Improving network and information security in the EU" ran from 23 July to 15 October 2012

² Eurobarometer 390/2012

changing landscape of threats and to ensure a common high level of protection in all the Member States.

Despite the initiatives undertaken, the Member States have very different levels of capabilities and preparedness, leading to fragmented approaches across the Union. This situation is not only detrimental to NIS in those Member States with a high level of protection. It also hinders the creation of trust among peers, which is a prerequisite for cooperation and information sharing. As a result, cooperation is taking place only amongst a minority of Member States with a high level of capabilities.

Therefore, there is currently no effective mechanism at EU level for effective cooperation and collaboration and for trusted information sharing on NIS incidents and risks amongst the Member States. This may result in uncoordinated regulatory interventions, incoherent strategies and divergent standards, meaning insufficient protection against NIS incidents and risks across the EU. It can also give rise to Internal Market barriers generating compliance costs for companies operating in more than one Member State.

Finally, there are no appropriate obligations placed on all players managing critical infrastructure or providing services that are essential to the functioning of our societies to adopt risk-management measures and exchange information with relevant authorities. Businesses therefore on the one hand lack effective incentives to conduct serious risk management, involving risk assessment and the adoption of appropriate steps to ensure NIS. On the other hand, a large proportion of incidents do not reach the competent authorities and go unnoticed; whereas information on incidents is essential for public authorities to react and take the appropriate mitigating measures, and set the adequate NIS strategic priorities.

The current regulatory framework requires only telecommunication companies to adopt risk management steps and to report serious NIS incidents. However, many other sectors rely on ICT as an enabler and should therefore be concerned about NIS as well. A number of specific infrastructure and service providers are particularly vulnerable, due to their high dependence on correctly functioning network and information systems. These sectors play an essential role in providing key support services for our economy and society and the security of their systems is of particular importance to the functioning of the Internal Market. These sectors include banking, stock exchanges, energy generation, transmission and distribution, transport (air, rail, maritime), health, important Internet companies enabling other online services and public administrations.

A step-change is therefore needed in the way NIS is dealt with in the EU. Regulatory obligations are required to create a level playing field and close existing legislative loopholes. To address these problems and increase the level of NIS within the European Union, the objectives of the proposed Directive are as follows.

First, the proposal requires all the Member States to ensure to have in place a minimum level of national capabilities by setting up competent authorities for NIS and Computer Emergency Response Teams (CERT), as well as by adopting a national NIS strategies and national NIS cooperation plans.

Secondly, the national competent authorities would cooperate within a network enabling secure and effective coordination, including coordinated information exchange as well as detection and response at Union level. Through this network, Member States would exchange information and cooperate to counter NIS threats and incidents on the basis of the European NIS cooperation plan.

Thirdly, based on the model of the Framework Directive for electronic communications, the proposal would aim to ensure that a culture of risk management develops and that sharing of

information between the private and public sectors takes place. Companies in the specific critical sectors outlined above and public administrations would be required to assess the risks they face and adopt appropriate and proportionate measures to ensure NIS. These entities would be required to report to competent authorities incidents seriously compromising their networks and information systems and having a significant impact on the continuity of services and supply of goods.

1.2. General Context

Over the last decade, economic growth and societal welfare have become increasingly dependent on the smooth functioning of digital networks and information systems. In Europe, the ICT sector and investments in ICT deliver around half of our productivity growth. The ICT sector alone represents almost 6% of the European GDP. Each year, 40% of all European citizens buy products and services over the Internet. 27% of European enterprises purchase and 13% sell online. As the main digital communications artery, Internet and information systems play an increasingly key role in the completion of the European Internal Market by facilitating the cross-border movement of goods, services and people.

Already in 2001, in its Communication "Network and Information Security: Proposal for A European Policy Approach", the Commission outlined the increasing importance of NIS for our economies and societies³. This was followed by the adoption in 2006 of a Strategy for a Secure Information Society⁴ aiming at developing a culture of network and information security in Europe based on dialogue, partnership and empowerment. Its main elements were endorsed in a Council Resolution⁵.

The Commission further adopted, on 30 March 2009, a Communication on Critical Information Infrastructure protection (CIIP)⁶ focusing on the protection of Europe from cyber disruptions by enhancing security and resilience. The Communication launched an action plan promoting Member States' efforts to ensure preparedness and prevention, detection and response, as well as mitigation and recovery. The Action plan was endorsed in the Presidency Conclusions of the Ministerial conference on CIIP in Tallinn in 2009. On 18 December 2009 the Council adopted a Resolution on "A collaborative European approach to network and information security"⁷.

The Digital Agenda for Europe⁸ (DAE), adopted in May 2010, and the related Council Conclusions⁹, highlighted the shared understanding that trust and security are fundamental pre-conditions for the wide uptake of ICT and therefore for achieving the objectives of the "smart growth" dimension of the Europe 2020 Strategy¹⁰. Under its Trust and Security chapter, the DAE emphasised the need for all stakeholders to join forces in a holistic effort to ensure the security and resilience of ICT infrastructure, by focusing on prevention, preparedness and awareness, as well as to develop effective and coordinated security mechanisms. In particular, key action 6 of the Digital Agenda for Europe calls for measures aimed at a reinforced and high-level NIS policy.

³ COM(2001)298

⁴ COM(2006)251 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf

⁵ 2007/068/01

⁶ COM(2009)149

⁷ 2009/C 321/01

⁸ COM(2010) 245

⁹ Council Conclusions of 31 May 2010 on Digital Agenda for Europe (10130/10)

¹⁰ COM(2010) 2020 and Conclusions of the European Council of 25/26 March 2010 (EUCO 7/10)

The DAE is complementary to other initiatives such as the Stockholm Programme for Freedom, Security and Justice and the Internal Security Strategy in action (ISS)¹¹. The Stockholm Programme/Action Plan¹² and the ISS underline the Commission's commitment to building a digital environment where every European can fully express their economic and social potential.

In its Communication on CIIP of March 2011 on "Achievements and next steps: towards global cyber-security"¹³, the Commission took stock of the results achieved since the adoption of the CIIP action plan in 2009, concluding that the implementation of the Plan showed that purely national approaches to tackle the security and resilience challenges are not sufficient, and that Europe should continue its efforts to build a coherent and cooperative approach across the EU. The 2011 CIIP Communication announces 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 have not yet been implemented.

In its Conclusions on CIIP of 27 May 2011¹⁴ the Council of the European Union stressed the pressing need to make ICT systems and networks resilient and secure to all possible disruptions, whether accidental or intentional; to develop across the Union a high level of preparedness, security and resilience capabilities and to upgrade technical competences to allow Europe to face the challenge of network and information infrastructure protection; and to foster cooperation between the Member States by developing incident cooperation mechanisms between the Member States.

1.3. Existing European Union and international provisions in this area

Under Regulation (EC) No 460/2004, the European Community established in 2004 the European Network and Information Security Agency (ENISA)¹⁴, with the purpose of contributing to the goals of ensuring a high level of network and information security within the Union and developing a culture of network and information security for the benefit of citizens, consumers, enterprises and public administrations. Its role 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. A proposal to modernise the mandate of ENISA was adopted on 30 September 2010¹⁵ and is under discussion in the Council and the European Parliament. The proposed Directive foresees that the Agency supports the cooperation mechanisms set out therein by providing its expertise and advice. .

The revised regulatory framework for electronic communications¹⁶ in force since November 2009 imposes security obligations on electronic communication providers¹⁷. These obligations had to be transposed at national level by May 2011.

All players who are data controllers (for example banks or hospitals) are obliged by the data protection regulatory framework¹⁸ to put in place security measures to protect personal data. Also, according to the 2012 Commission proposal for General Data Protection Regulation¹⁹, data controllers would have to report breaches of personal data to the national supervisory

¹¹ COM(2010)673 [lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF)

¹² COM(2010)171 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:EN:PDF>

¹³ COM(2011)163

¹⁴ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML> and

¹⁵ COM(2010) 521

¹⁶ See http://ec.europa.eu/information_society/policy/ecomms/doc/library/regframeforec_dec2009.pdf

¹⁷ Art. 13a&b of the Framework Directive

¹⁸ Directive 2002/58 of 12 July 2002.

¹⁹ COM(2012) 11

authorities. This means that, for example, a NIS security 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) would not have to be notified.

Under Directive 2008/114 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, the "European Programme for Critical Infrastructure Protection (EPCIP)"²⁰ sets out the overall "umbrella" approach to the protection of critical infrastructures in the EU. The objectives of EPCIP are fully consistent with this proposal and the Directive should apply without prejudice to Directive 2008/114. EPCIP does not place obligations on operators to report significant breaches of security and does not set up mechanisms for the Member States to cooperate and respond to incidents.

The co-legislator is currently discussing the Commission proposal for a Directive on attacks against information systems²¹ which aims at harmonising the criminalisation of specific conducts. This proposal covers only the criminalisation of specific conducts, but does not address the prevention of NIS risks and incidents, the response to NIS incidents and the mitigation of their impact. This Directive should apply without prejudice to the Directive on attacks against information systems.

On 28 March 2012, the Commission adopted a Communication²² on the establishment of a European Cybercrime Centre (EC3)²³. This Centre will be part of the European Police Office (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 the 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, the EU works on cybersecurity both at bilateral and multilateral level. At the occasion of the 2010 EU-US Summit²⁴, the EU-US Working Group on Cybersecurity 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 in the global debate on the development of norms of responsible behaviour in cyberspace and on confidence building measures.

2. RESULTS OF CONSULTATIONS WITH THE INTERESTED PARTIES AND IMPACT ASSESSMENTS

2.1. Consultation with interested parties and use of expertise

An online public consultation on "Improving NIS in the EU" ran between 23 July and 15 October 2012. In total, the Commission received 160 responses to the online questionnaire.

The key outcome was that stakeholders showed general support for the need to improve NIS across the EU. In particular, 82.8% of the respondents expressed the view that governments in the EU should do more to ensure a high level of NIS; 82.8% were of the opinion that users of

²⁰ COM(2006)786 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf

²¹ COM(2010) 517, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF>

²² COM(2012)140 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF>

²³ COM(2012)140 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF>

²⁴ http://europa.eu/rapid/press-release_MEMO-10-597_en.htm

information and systems are unaware of the existing NIS threats and incidents; 66.3% of respondents would in principle be in favor of the introduction of a regulatory requirement to manage NIS risks and 84.8% said that such requirements should be set at EU level. A high number of respondents estimated that it would be important to adopt NIS requirements in particular in the following sectors: banking and finance (91.1%), energy (89.4%), transport (81.7%), health (89.4%), Internet services (89.1%), public administrations (87.5%). Respondents also 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%). Finally, respondents affirmed 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%); and that a requirement to report security breaches would not cause significant additional costs (52.5%) or not additional costs at all (19.8%).

Consultation with the Member States took place in a number of relevant Council configurations; in the context of the European Forum for Member States (EFMS)²⁵; at the occasion of the Conference on Cybersecurity organised by the Commission and the European External Action Service on 6 July 2012; and in dedicated bilateral meetings convened at the request of individual Member States.

Discussions with the private sector also took place in the framework of the European Public-Private Partnership for Resilience²⁶ and through bilateral meetings. As for the public sector, the Commission held discussions with ENISA and the CERT for the EU institutions.

A discussion with the general public was organised in the context of the 2012 Digital Agenda Assembly²⁷.

2.2. Impact assessment

The Commission has carried out an impact assessment of three Policy options:

Option 1: Business as usual (Baseline scenario): maintaining the current approach;

Option 2: Regulatory approach, consisting of a legislative proposal establishing a common EU legal framework on NIS regarding Member States capabilities, mechanisms for EU-level cooperation, and requirements for key private players and public administrations;

Option 3: Mixed approach, by combining voluntary initiatives on the Member States NIS capabilities and mechanisms for EU-level cooperation with regulatory requirements for key private players and public administrations.

The Commission concluded that Option 2 would have the strongest positive impacts, as under this Option the protection of EU consumers, business and governments against NIS incidents, threats and risks would improve considerably. In particular, the obligations placed on the Member States would ensure adequate preparedness at national level, and would contribute to a climate of mutual trust, which is a precondition for effective cooperation at EU level. The setting up of mechanisms for cooperation at EU level via the network would deliver coherent and coordinated prevention and response to cross-border NIS incidents and risks. The introduction of requirements to carry out NIS risk management for public administrations and key private players would create a strong incentive to manage security risks effectively. The obligation to report NIS incidents with a significant impact would enhance the ability to respond to incidents and foster transparency. 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

²⁵

²⁶ <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r>

²⁷ Final report: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/daa12-final_report_1.pdf

for cooperation at bilateral and multilateral level. The EU would hence also be better placed to promote fundamental rights and EU core values abroad.

The quantitative assessment showed that Option 2 would not impose a disproportionate burden to the Member States. The costs for the private sector would also be limited since many of the affected entities 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). Existing spending on security in the private sector has also been taken into account.

Option 1 and 3 were not considered viable for reaching the policy objectives and are therefore not recommended, given that their effectiveness would depend on whether the voluntary approach would actually deliver a minimum level of NIS. Also, the effectiveness of Option 3 would depend on the goodwill of the Member States to strengthen their capabilities and cooperate cross-border.

3. LEGAL ELEMENTS OF THE PROPOSAL

3.1. 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). Under Article 114 TFEU, the Union can adopt "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".

As indicated above, network and information systems play an essential role in facilitating the cross-border movement of goods, services and people. They are often interconnected and the Internet has a global nature. Given this intrinsic transnational dimension, a disruption in one Member State can also affect other Member States and the EU as a whole. The resilience and stability of network and information systems is therefore essential to the smooth functioning of the Internal Market.

The EU legislator has already recognised the need to harmonise NIS rules to ensure the development of the internal market. In particular, this was the case for Regulation 460/2004/EC establishing ENISA²⁸ which is based on Article 114 TFEU.

The disparities resulting from uneven NIS national capabilities, policies and level of protection across the Member States lead to barriers to the internal market and justify EU action.

3.2. Subsidiarity

European intervention in the area of NIS is justified by the subsidiarity principle.

Firstly, considering the cross-border nature of NIS, non-intervention at EU level would lead to a situation where each Member State would act alone disregarding the interdependences among EU network and information systems. An appropriate degree of coordination among the Member States would ensure that NIS risks can be well managed in the cross-border context in which they arise. Divergences in NIS regulations represent a barrier for companies to operate in multiple countries and to the achievement of global economies of scale.

²⁸ 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).

Secondly, regulatory obligations at EU level are needed to create a level playing field and close legislative loopholes. A purely voluntary 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 involving all the Member States it is necessary to ensure that they all have the required minimum level of capability. NIS measures adopted by governments need to be consistent with each other and coordinated to contain and minimise the consequences of NIS incidents. In addition, 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. Action at EU level would therefore improve the effectiveness and facilitate the development of existing national policies.

The proposed measures are also justified on grounds of proportionality. The requirements for the Member States are set at the minimum level necessary to achieve adequate preparedness and to enable cooperation based on trust. The requirements to carry out risk management target only critical entities and impose measures that are proportionate to the risks. The public consultation underlined the importance of ensuring the security of these critical entities. The reporting requirements would concern only incidents with a significant impact. As indicated above, the measures would not impose disproportionate costs, as many of these entities as data controllers are already required by the current data protection rules to secure the protection of personal data.

The stated objectives can be better achieved at EU level, rather than by the Member States alone, in view of the cross-border aspects of NIS incidents and risks. Therefore, the EU may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, the proposed Directive does not go beyond what is necessary in order to achieve those objectives.

For the purpose of achieving the objectives, the Commission should be empowered to adopt delegated acts in accordance with Article 290 of the Treaty on the Functioning of the European Union, in order to supplement or amend certain non-essential elements of the basic act.

In order to achieve uniform conditions for the implementation of the basic act, the Commission should be empowered to adopt implementing acts in accordance with Article 291 of the Treaty on the Functioning of the European Union.

4. BUDGETARY IMPLICATION

The cooperation and exchange of information between Member States would be supported by a secure infrastructure. The proposal would have EU budgetary implications only if Member States choose to adapt an existing infrastructure (e.g. sTESTA) and task the Commission to implement the adaptation under the MFF 2014-2020. The related one-off cost is estimated to be 1 250 000 million EUR and would 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 sufficient funds are available under CEF. Alternatively Member States can either share the one-off cost of the adaptation of an existing infrastructure or decide to set up a new infrastructure and bear the costs, which are estimated to be approximately 10 million EUR per year.

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

Having regard to the opinion of the European Economic and Social Committee,

Having regard to the opinion of the Committee of the Regions,

After transmission of the draft legislative act to the national Parliaments,

[After consulting the European Data Protection Supervisor]

Acting in accordance with the ordinary legislative procedure,

Whereas:

- (1) Network and information systems and services play a vital role in European society. Their reliability and security is essential to economic activities and social welfare, and in particular for the functioning of the internal market.
- (2) The magnitude and frequency of deliberate or accidental security incidents is increasing and represents a major threat to the functioning of networks and information systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.
- (3) As a communication instrument without frontiers, digital information systems, and primarily the Internet play an essential role in facilitating the cross-border movement of goods, services and people. Due to this transnational nature, substantial disruption in one Member State can also affect other Member States and the EU as a whole. The resilience and stability of network and information systems is therefore essential to the smooth functioning of the Internal Market.
- (4) A cooperation mechanism should be established at Union level to allow for information exchange and coordinated detection and response regarding network and information security ("NIS"). For this mechanism to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of security in their territory. Minimum security requirements should also apply to public administrations and operators of critical information infrastructure to promote a culture of risk management and ensure that the most serious incidents are reported.
- (5) To cover all security incidents and risks, this Directive should apply to all network and information systems. The obligations on public administrations and market

players should however not apply to providers of electronic communications networks and electronic communications services within the meaning of Directive 2002/21/EC, which are subject to the specific security and integrity requirements laid down in Article 13a of this Directive nor should they apply to trust service providers within the meaning of the Commission's proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

- (6) The existing capabilities are insufficient to ensure a high level of NIS within the Union. Member States have very different levels of preparedness leading to fragmented approaches across the Union. This leads to an unequal level of protection of consumers and businesses, and undermines the overall level of network and information security within the Union. Lack of common minimum requirements on Member States and market operators in turn makes it impossible to set up a global and effective mechanism for cooperation at Union level.
- (7) Responding effectively to the challenges of the security of network and information systems therefore requires a holistic approach at Union level covering common minimum capacity building and planning requirements; exchange of information and coordination of actions; and common minimum security requirements for all market operators concerned and public administrations.
- (8) The provisions of this Directive are without prejudice to the possibility for each Member State to take the necessary measures to ensure the protection of its essential security interests, to safeguard public policy and public security, and to permit the investigation, detection and prosecution of criminal offences. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security.
- (9) To achieve and maintain a common high level of security of network and information systems, each Member State should have a national NIS security strategy defining the strategic objectives and concrete policy actions to be implemented. NIS cooperation plans complying with essential requirements need to be developed at national level in order to reach capacity response levels allowing for effective and efficient cooperation at national and Union level in case of incidents.
- (10) To allow for the effective implementation of this Directive, a body responsible for coordinating network and information security issues and acting as a focal point for cross-border cooperation at Union level should be established or identified in each Member State. These bodies should be given the adequate technical, financial and human resources to ensure that they can carry out in an effective and efficient manner the tasks assigned to them and thus achieve the objectives of this Directive.
- (11) All Member States should be adequately equipped, both in terms of technical and organisational capabilities, to prevent, detect, respond and mitigate network and information systems' security incidents and risks . Well-functioning Computer Emergency Response Teams complying with essential requirements should therefore be established in all Member States to guarantee effective and compatible capabilities to handle security incidents and ensure efficient cooperation at Union level.
- (12) Building upon the significant progress made by the European Forum of Member States (EFMS) in fostering discussions and exchanges on good policy practices, the Member States and the Commission should form a network to bring them into

permanent communication and support their cooperation. This secure and effective cooperation mechanism should enable structured and coordinated information exchange, detection and response at Union level.

- (13) The European Network and Information Security Agency (ENISA) should assist the Member States and the Commission by providing its expertise and advice and by facilitating exchange of best practices.
- (14) To ensure effective and timely information to the Member States and the Commission, early warnings on network and information systems incidents and risks that have an actual or potential Union dimension should be notified within the network of competent authorities. To build capacity and knowledge among Member States, the network should also serve as an instrument for the exchange of best practices, assisting its members in building capacity, steering the organisation of peer reviews and NIS exercises.
- (15) A secure information-sharing infrastructure should be put in place to allow for the exchange of sensitive and confidential information within the network. Without prejudice to their obligation to notify incidents and risks of Union dimension to the network of competent authorities, access to confidential information from other Member States should only be granted to Member States upon demonstration that their technical, financial and human resources and processes, as well as their communication infrastructure, guarantee their effective, efficient and secure participation in the network.
- (16) As most network and information systems are privately operated, cooperation between the public and private sectors is essential. Industry players should be encouraged to pursue their own informal cooperation mechanisms to ensure network and information security. They should also cooperate with the public sector, share information and best practices in exchange of operational support in case of security incidents.
- (17) The competent authorities shall set up a common website to publish non confidential information on the incidents and risks.
- (18) Where information is considered confidential in accordance with Union and national rules on business confidentiality, such confidentiality shall be ensured when carrying out the activities and fulfilling the objectives set by this Directive.
- (19) On the basis in particular of national crisis management experiences and in cooperation with ENISA, the Commission and the Member States should develop a NIS security cooperation plan defining cooperation mechanisms to counter risks and incidents. This Plan should be duly taken into account in the operation of early warnings within the network.
- (20) The notification of an early warning within the network should be required only where the scale and severity of the incident or risk concerned are or may become so significant that information or coordination of the response at the Union level is necessary. Early warnings should therefore be limited to actual or potential incidents or risks that grow rapidly, exceed national response capacity or affect more than one Member State. To allow for a proper evaluation, all information relevant for the assessment of the risk or incident should be communicated to the network.
- (21) Upon receipt of an early warning and its assessment, the competent authorities should agree on a coordinated response under the European NIS cooperation plan.

All competent authorities should be informed about the measures adopted at national level as a result of the coordinated response.

- (22) Responsibilities in ensuring network and information security lie to a great extent on public administrations and market operators. A culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced should be promoted and developed through appropriate regulatory requirements and voluntary industry practices. Establishing a level playing field is also essential for the effective functioning of the network.
- (23) Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) requires that providers of public electronic communications networks or publicly available electronic communications services take appropriate measures to safeguard their integrity and security and introduces security breach and integrity loss notification requirements²⁹. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) requires a provider of a publicly available electronic communications service to take appropriate technical and organisational measures to safeguard the security of its services.
- (24) These obligations should be extended beyond the electronic communications sector to key providers of information society services, such as e-commerce platforms or cloud computing service providers, which underpin downstream information society services or on-line activities, such as e-commerce or social networking; and to public administrations and operators of critical infrastructure, which rely heavily on ICT and are essential for the maintenance of vital economical or societal functions such as electricity and gas, transport, credit institutions, stock exchange, health. Disruption of those network and information systems would affect the internal market.
- (25) The public administrators and private actors should ensure security of the networks and systems which are under their control. These will be primarily private networks and systems managed either by their internal IT staff or the security of which has been outsourced. These will exclude public electronic communications networks which are beyond their control, which should continue to be covered by Directive 2002/21/EC.
- (26) To avoid imposing a disproportionate financial and administrative burden on small operators and users, the requirements should be proportionate to the risk presented by the network or information system concerned, taking into account the state of the art of such measures. These requirements should not apply to micro enterprises.
- (27) Competent authorities should pay due attention to preserving informal and trusted channels of information-sharing between private operators and between the public and the private sectors. Publicity of security incidents reported to the competent authorities should duly balance the interest of the public in being informed about

²⁹ Art. 13a&b of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (the Framework Directive). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

threats with possible reputational and commercial damages for the private actors reporting security incidents.

- (28) Competent authorities should have the necessary means to perform their duties, including powers to obtain sufficient information from market operators in order to assess the level of security of network and information systems as well as reliable and comprehensive data about actual security incidents that have had an impact on the operation of network and information systems.
- (29) National regulatory authorities created pursuant to Directive 2002/21/EC and the competent authorities established under this Directive should closely cooperate and provide each other with the information necessary for the effective implementation of Directive 2002/21/EC and of this Directive.

Criminal activities are in many cases underlying a security incident. The criminal nature of incidents can be suspected even if the evidence to support it may not be sufficiently clear from the start. In this context, appropriate co-operation between competent authorities and law enforcement authorities should form part of an effective and comprehensive response to the threat of security incidents. In particular, promoting a safe, secure and more resilient environment requires a systematic reporting of incidents of a suspected serious criminal nature to law enforcement authorities. Under [Directive 2012/XX of the European Parliament and of the Council of [] on attacks against information systems and replacing Council Framework Decision 2005/222/JHA], Member States will determine what constitutes incidents of a serious criminal nature, such as major attacks against information systems disrupting system services of significant public importance, or causing major financial cost or loss of personal data or sensitive information.

- (30) Standardisation is a market-driven process. However there might be situations where it is appropriate to require compliance of conformity with specified standards to ensure a high level of security at Union level.
- (31) Network and information systems' security problems are global issues. There is a need for closer international cooperation to improve security standards and information exchange, and promote a common global approach to network and information security issues.
- (32) The power to adopt delegated acts in accordance with Article 290 of the Treaty on the functioning of the European Union should be conferred to the Commission for the definition of the triggering events for early warning, the specification of security requirements, and the circumstances in which providers and public administrations are required to notify security breaches.
- (33) It is of particular importance that the Commission carries out appropriate consultations during its preparatory work, including at expert level, as far as the urgency of the situation allows it. The Commission, when preparing and drawing up delegated acts, should ensure simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.
- (34) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission to adopt implementing acts in relation to the functioning of the cooperation network; and to recommend standards and/or technical specifications on network and information security. Those implementing powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying

down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers³⁰.

- (35) Classified information should be protected in accordance with relevant Union and Member State legislation. Each Member State and the Commission should respect the relevant security classification given by the originator of a document.
- (36) Information that is considered confidential by a competent authority, in accordance with Union and national rules on business confidentiality, may be exchanged with the Commission and other competent authorities only where such exchange is strictly necessary for the application of the provisions of this Directive. The information exchanged should be limited to that which is relevant and proportionate to the purpose of such an exchange.
- (37) The processing of personal data for the purpose of implementing this Directive should comply with 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 data³¹, and with Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector³². The implementation of this Directive shall in particular be without prejudice to the fundamental right of individuals to be informed about the processing of their personal data.
- (38) The sharing of information on network and information security risks and incidents within the cooperation network of the Member States and compliance with the requirement to notify incidents to the national competent authorities may require the processing of personal data. In this case the processing will be necessary to comply with a legal obligation and thus be legitimate according to Directive 95/46/CE.
- (39) The processing of personal data for the purpose of implementing this Directive should comply with Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data³³.
- (40) In the application of this Directive, Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents should apply as appropriate.
- (41) Since the objectives of this Directive, namely to ensure a high level of network and information security in the Union, cannot be sufficiently achieved by the Member States alone and can therefore, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.
- (42) The Commission should periodically review this Directive, in particular with a view to determining the need for modification in the light of changing technological or market conditions.

³⁰ OJ L 55, 28.2.2011, p.13.

³¹ OJ L 281, 23.11.1995, p. 31.

³² OJ L 201, 31.7.2002, p. 37.

³³ OJ L 8, 12.1.2001, p. 1.

- (43) This Directive is in full respect of the fundamental rights, and observes the principles, recognised in particular by the Charter of Fundamental Rights of the European Union. Measures taken in the application of this Directive should respect and observe those fundamental rights and principles, as well as general principles of Union law.

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This Directive lays down measures to ensure a high common level of network and information systems security (hereinafter referred to as "NIS") within the Union, which is essential for the smooth functioning of the internal market.
2. To this end, this Directive:
 - (a) provides for obligations for all Member States concerning the prevention, the handling of and the response to security risks and incidents;
 - (b) creates a cooperation mechanism between Member States in order to ensure a uniform application of this Directive within the Union and, where necessary, a coordinated and efficient handling of and response to security risks and incidents;
 - (c) establishes security requirements for market operators and public administrations.
3. The security requirements do not apply to providers of electronic communications networks and electronic communications services within the meaning of Directive 2002/21/EC, which shall comply with the specific security and integrity requirements laid down in Article 13a and b of that Directive, and to trust service providers within the meaning of the Commission's proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
4. This Directive shall be without prejudice to [Directive 2012/XX of the European Parliament and of the Council of [] on attacks against information systems and replacing Council Framework Decision 2005/222/JHA], and Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection as well as to the Critical Infrastructure Warning Information Network (CIWIN).
5. This Directive shall also be without prejudice to Directive 95/46/CE 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 data³⁴, and to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. The requirements to share information within the cooperation network in chapter III and to notify NIS incidents under Article 14 this Directive shall constitute legal requirements for processing personal data according to Article 7(c) of Directive 95/46/CE.

Article 2

³⁴ OJ L 281 , 23/11/1995 p. 31.

Minimum harmonisation

Member States shall not be prevented from adopting or maintaining provisions ensuring a higher level of security, without prejudice to their obligations under the Treaty.

Article 3

Definitions

For the purpose of this Directive, the following definitions shall apply:

- (a) "Network and information system" means an electronic communications network within the meaning of Directive 2002/21/EC and any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance;
- (b) "Security" means the ability of a network or information system to resist, at a given level of confidence, accident 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;
- (c) "Risk" means any circumstance or event having a potential adverse effect on security;
- (d) "Incident" means any circumstance or event having an actual adverse effect on security;
- (e) "Information society services" mean services within the meaning of Directive Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC;
- (f) "NIS cooperation plan" means a plan establishing the framework for organisational roles, responsibilities and procedures to maintain or restore the operation of networks and information systems, in the event of emergency, incident or disaster;
- (g) "Incident handling" means all procedures supporting the analysis, containment and response to an incident;
- (h) "Preparedness" means a state of readiness and capability of human and material means enabling them to ensure an effective rapid response to an emergency, obtained as a result of action taken in advance;
- (i) "Market operators" means:
 - Providers of information society services which enable the provision of other information society services or of on-line activities as indicated in Annex IV; and
 - Operators of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health as indicated in Annex IV.
- (j) "European standard" means a standard adopted by a European standardisation organisation.
- (k) "Harmonised standard" means a European standard adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation.
- (l) "Technical specification" means a document that prescribes technical requirements.

- (m) "ICT Technical specification" means a technical specification in the field of information and communication technologies.

CHAPTER II

NATIONAL FRAMEWORKS ON NETWORK AND INFORMATION SECURITY

Article 4

Principle

Member States shall ensure a high level of security of the network and information systems in their territories in accordance with this Directive.

Article 5

National NIS strategy

1. Each Member State shall have, no later than one year from the entry into force of this Directive, a national NIS strategy defining the strategic objectives and concrete policy and regulatory measures to achieve and maintain a high level of network and information security. The national NIS strategy shall address in particular the issues set out in Annex I.
2. The national NIS strategy shall include a national NIS cooperation plan complying with the minimum requirements set out in Annex II.
3. The national NIS strategy and the national NIS cooperation plan shall be communicated to the Commission.

Article 6

National competent authority on the security of network and information systems

4. Each Member State shall designate a national competent authority on the security of network and information systems (the "competent authority").
5. The competent authorities shall monitor the application of this Directive at national level and contribute to its consistent application throughout the Union.
6. Member States shall ensure that the competent authorities have adequate technical, financial and human resources to carry out in an effective and efficient manner the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure the effective, efficient and secure cooperation of the competent authorities via the network referred to in Article 8.
7. Member States shall ensure that the competent authorities receive the notifications of incidents from public administrations and market operators as specified under Article 14(2) and are granted the implementation and enforcement powers referred to under Article 15.
8. The competent authorities shall consult and cooperate, whenever appropriate, with the relevant law enforcement national authorities.
9. Each Member State shall notify to the Commission without delay the designation of the competent authority, its tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent authority.

Article 7

Computer Emergency Response Team (CERT)

10. Each Member State shall set up a CERT responsible for handling security incidents and risks according to a well-defined process, which shall comply with the essential requirements set out in Annex III(1). A CERT may be established within the competent authority.
11. Member States shall ensure that CERTs have adequate technical, financial and human resources to carry out their tasks, as indicated in Annex III(2), effectively.
12. Member States shall ensure that CERTs rely on a secure and resilient communication and information infrastructure at national level, which shall be compatible and interoperable with the secure information-sharing system of the network referred to in Article 9.
13. Member States shall inform the Commission about the resources and mandate as well as the incident handling process of the CERTs.
14. The CERT shall act under the supervision of the competent authority, which shall regularly review the adequacy of its resources, its mandate and the effectiveness of its incident-handling process.

CHAPTER III

COOPERATION BETWEEN COMPETENT AUTHORITIES

Article 8

Cooperation network

1. The competent authorities and the Commission shall form a network to cooperate against NIS risks and threats.
2. The network shall bring into permanent communication the Commission and the competent authorities. When requested, the European Network and Information Security Agency (ENISA) shall assist the network by providing its expertise and advice.
3. Within this network the competent authorities shall:
 - (a) circulate early warnings on security risks and incidents affecting network and information systems in accordance with Article 10.
 - (b) ensure a coordinated response in accordance with Article 11; and regular publication of non confidential information on on-going early warnings and coordinated response on a common website.
 - (c) jointly discuss and assess, at the request of one Member State or of the Commission, one or more national NIS strategies and national NIS cooperation plans referred to in Article 5, within the scope of this Directive.
 - (d) jointly discuss and assess, at the request of a Member State or the Commission, the effectiveness of the CERTs, in particular when NIS exercises are performed at Union level.
 - (e) cooperate and exchange information with the Europol Cybercrime Center, and with other relevant European bodies in particular in the fields of data protection, energy, transport, banking, stock exchanges and health; exchange information and best practices between themselves and the Commission, and assist each other in building capacity on NIS;
 - (f) organise regular peer reviews on capabilities and preparedness;

- (g) organise NIS exercises at Union level and participate, as appropriate, in international NIS exercises.

The Commission shall by means of implementing acts establish the necessary modalities to facilitate the cooperation between competent authorities and the Commission referred to in paragraphs 2 and 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 18(2).

Article 9

Secure information-sharing system

1. The exchange of sensitive and confidential information within the network shall take place through a secure infrastructure.
2. The Commission shall be empowered to adopt by means of implementing acts, decisions on the access of the Member States to this secure infrastructure. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 18(3).
3. The Commission's decision shall be based on the assessment by the Commission, with the assistance of ENISA, of the adequate transposition by the Member States of Chapter II of this Directive, and in particular:
 - of the availability of a secure and resilient communication and information infrastructure at national level, compatible and interoperable with the secure infrastructure of the network in compliance with Article 7(3), and
 - that their competent authority and CERT have adequate technical, financial and human resources and processes to guarantee their effective, efficient and secure participation in the network in compliance with Article 6(3), 7(2) and 7(3).

Article 10

Early warnings

4. The competent authorities or the Commission shall provide early warnings within the network on those risks and incidents that fulfil at least one of the following conditions:
 - (a) They grow rapidly or may grow rapidly in scale;
 - (b) They exceed or may exceed national response capacity;
 - (c) They affect or may affect more than one Member State.
5. In the early warnings, the competent authorities and the Commission shall communicate any relevant information in their possession that may be useful for assessing the risk or incident.
6. At the request of a Member State, or on its own initiative, the Commission may request a Member State to provide any relevant information on a specific risk or incident.
7. Where the risk or incident subject to an early warning is of a suspected criminal nature, the competent authorities or the Commission shall inform the Europol Cybercrime Center.

Article 11
Coordinated response

1. Following an Early Warning the Competent Authorities shall, after assessing the relevant information, agree on a coordinated response under the European NIS cooperation plan.
2. The various measures adopted at national level as a result of the coordinated response shall be communicated to the network.

Article 12
NIS cooperation plans

3. The Commission shall be empowered to adopt by means of implementing acts a plan setting out the modalities and the operational rules on the network, after consulting ENISA. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 18(3).
4. The operational rules shall include:
 - (a) a definition of the risks and incidents triggering early warnings under Article 10;
 - (b) a definition of the format and procedures under Article 10 for:
 - the collection and sharing of compatible and comparable data on risks and incidents by the competent authorities,
 - the criteria for the assessment of the threats and incidents by the network.
 - (c) the processes to be followed for the coordinated responses under Article 11, including identification of roles and responsibilities and cooperation procedures;
 - (d) a roadmap for NIS exercises and training to reinforce, validate, and test the plan;
 - (e) a programme for transfer of knowledge between the Member States in relation to capacity building and peer learning;
 - (f) a programme for awareness raising and training between the Member States.
5. The operational rules on the functioning of the network shall be adopted no later than [one year] following the entry into force of this Directive and shall be revised regularly.

Article 13
International cooperation

Without prejudice to the possibility for the network to have informal international cooperation, the Union may conclude international agreements with third countries or international organisations allowing and organizing their participation in some activities of the network.

CHAPTER IV
SECURITY OF THE NETWORKS AND INFORMATION SYSTEMS OF PUBLIC
ADMINISTRATIONS AND MARKET OPERATORS

Article 14

Security requirements and incident notification

1. Member States shall ensure that public administrations and market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of security incidents affecting their network and information system on the services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.
2. Member States shall ensure that public administrations and market operators notify to the competent authority incidents having a significant impact on the services they provide.
3. The competent authority may inform the public or require the public administrations and market operators to do so, where it determines that disclosure of the incident is in the public interest. Once a year, the competent authority shall submit a summary report to the network on the notifications received and the action taken in accordance with this paragraph.
4. The Commission shall be empowered to adopt, where relevant, delegated acts in accordance with Article 17 concerning the circumstances in which providers are required to notify security breaches.
5. Subject to any delegated act adopted under paragraph 4, the competent authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which providers are required to notify security breaches.
6. The Commission may, by means of implementing acts, define the formats and procedures applicable for the purpose of paragraph 3 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 18(3).
7. The measures taken by Member States for the specification of the security requirements referred to in paragraphs 1 and 2 shall be equivalent and compatible to the measures taken for the implementation of Article 13a of Directive 2002/21/EC.
8. Paragraphs 1 and 2 shall not apply to micro-enterprises as defined in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises³⁵.

Article 15

Implementation and enforcement

1. Member States shall ensure that in order to implement Article 14, competent authorities have the power to issue binding instructions to market operators.
2. Member States shall ensure that the competent authorities have the power to require market operators and public administrations to:
 - (a) provide information needed to assess the security of their networks and information systems, including documented security policies;
 - (b) submit to a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent

³⁵ OJ L 124/36 of 20 May 2003.

authority. The cost of the audit shall be paid by the relevant market operator or public administration.

3. Member States shall ensure that the competent authorities have all the powers necessary to investigate cases of non-compliance and the effects thereof on the security of networks and information systems.
4. The competent authorities shall notify incidents of a serious suspected criminal nature to law enforcement authorities.

Article 16

Standardisation

1. The Commission shall, by means of implementing acts, recommend to Member States for the implementation of Article 14(1) the use of standards and/or technical specifications (or reference numbers) relevant to network and information security, including, where relevant, harmonized standards, to serve as a basis for encouraging the coherent use of standardisation practises across the Union. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 18(2). The Commission shall publish those acts in the Official Journal of the European Union. Where appropriate, the Commission shall, in accordance with [Regulation (EU) No/2012 Regulation³⁶ request the European standards organisations (European Committee for Standardisation (CEN), European Committee for Electrotechnical Standardisation (CENELEC), and European Telecommunications Standards Institute (ETSI) to draw up European or harmonised standards.
2. Member States shall take utmost account of the Recommendation under paragraph 1 and encourage the use of the standards and/or technical specifications referred to in paragraph 1, to the extent strictly necessary to ensure network and information security.

CHAPTER V

FINAL PROVISIONS

Article 16a

Penalties

Member States shall lay down rules on penalties applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be appropriate, effective, proportionate and dissuasive. The Member States shall notify those provisions to the Commission by [] and shall notify it without delay of any subsequent amendment affecting them.

Article 17

Exercise of the delegation

1. The power to adopt the delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

³⁶ Regulation (EU) No/2012 of the European Parliament and of the Council on European standardisation

2. The power to adopt delegated acts referred to in Article 14(4) shall be conferred on the Commission. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.
3. The delegation of powers referred to in Article 14(4) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of the powers specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated act already in force.
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
5. A delegated act adopted pursuant to Article 14(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of 2 months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by 2 months at the initiative of the European Parliament or the Council.

Article 18

Committee

1. The Commission shall be assisted by a Committee (the "Network and Information Security Committee"). That Committee shall be a Committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 4 of Regulation (EU) No 182/2011 shall apply.
3. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 19

Review

The Commission shall periodically review the functioning of this Directive and report to the European Parliament and the Council. The first report shall be submitted no later than three years after the date of application referred to in Article 20. Subsequent reports shall be submitted every three years thereafter. For this purpose, the Commission may request information from the Member States, which shall be supplied without undue delay.

Article 20

Transposition

1. Member States shall adopt and publish by [] the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith communicate to the Commission the text of such provisions.

They shall apply those measures from [.]

When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 21

Entry into force

This Directive shall enter into force [on the day following its publication in the *Official Journal of the European Union*].

Article 22

Addressees

This Directive is addressed to the Member States.

Done at Brussels,

For the European Parliament
The President

For the Council
The President

ANNEX I

Items to be included in national NIS strategies

- (a) The definition of the objectives and priorities of the strategy based on an up-to-date risk and threat analysis;
- (b) A governance framework to achieve the strategy objectives and priorities, including a clear definition of the roles and responsibilities of the government bodies and the other relevant actors;
- (c) Identification of the measures on preparedness, response and recovery, including cooperation mechanisms between the public and private sectors;
- (d) Definition of the cooperation processes between the public and private sectors.
- (e) An indication of the education, awareness raising and training programmes;
- (f) Research and development plans and a description of how these plans reflect the identified priorities.

ANNEX II

Essential requirements for national NIS cooperation plans

- (a) A risk assessment plan to identify vulnerabilities and threats and assess the impacts of potential incidents;
- (b) Definition of the roles and responsibilities of the various actors involved in the implementation of the plan;
- (c) Definition of cooperation and communication processes ensuring prevention, detection, response, repair and recovery, and modulated according to the alert level;
- (d) A roadmap for NIS exercises and training to reinforce, validate, and test the plan. Lessons learned to be documented and incorporated into updates to the plan.

ANNEX III

Essential requirements and tasks of the Computer Emergency Response Team (CERT)

The essential requirements and tasks of the CERT shall be adequately and clearly defined and supported by national policy and/or regulation. They shall include the following elements.

1. Essential requirements for the Computer Emergency Response Team (CERT)

- The CERT shall ensure high availability of its communications services by avoiding single points of failure and have several means for being contacted and for contacting others. Furthermore, the communication channels should be clearly specified and well known to the constituency and cooperative partners.
- The CERT shall implement and manage security measures to ensure the confidentiality, integrity, availability and authenticity of information.
- The offices of the CERT and the supporting information systems must be located in secure sites.
- A service management quality system shall be created to follow-up on the performance of the CERT and ensure a steady process of improvement. This could be based on clearly defined metrics that include formal service levels and key performance indicators.
- Business continuity:
 - The CERT shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers.
 - The CERT shall be full-time staffed to ensure availability at all times.
 - The CERT shall rely on an infrastructure whose continuity is ensured. To this end, redundant systems and backup working space shall be set up for the CERT to ensure permanent access to the means of communication.

2. Tasks of the Computer Emergency Response Team (CERT)

- Services provided by the CERT shall include at least the following:
- Monitoring incidents at a national level
- Providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about security threats
- Responding to incidents
- Providing dynamic risk and incident analysis and situational awareness
- Building broad public awareness of the risks associated with online activities
- Campaigns on NIS security
- The CERT shall establish cooperative relationships with Private sector operators and providers.
- To facilitate cooperation, the CERT shall promote the adoption and use of common or standardised practises for:
 - incident and vulnerability handling procedures;
 - incident, vulnerability and information classification schemes;

- taxonomies for metrics;
- information exchange formats on vulnerabilities, incidents, and system naming conventions.

ANNEX IV

Indicative list of Market Operators

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 and/or gas Distribution System Operators (DSOs) and Retailers for final consumers
- Transmission System Operators (TSO) in natural gas, including storage, import into the country
- Transmission System Operators in electricity
- Electricity spot market
- For electricity generators, only the main players would be covered as possible NIS problems in energy supply affecting smaller generators would easily be tackled by other companies, whereas for transmission and distribution a NIS disruption could have an impact on customers regardless of the size of the company.

Transport

- Air carriers (Freight and passenger air transport)
- Maritime carriers (sea and coastal passenger water transport companies³⁷ and the number of sea and coastal freight water transport companies³⁸)
- Railways (infrastructure managers, integrated companies and railway transport operators)
- Airports (EU airports with more than 15.000 passenger unit movements per year)
- Ports
- Traffic management control operators
- Auxiliary logistics services (a) warehousing and storage³⁹, b) cargo handling⁴⁰ and c) other transportation support activities⁴¹)

Banking: credit institutions⁴²

Stock exchanges

Health sector: health care settings, including hospitals and private clinics

³⁷ NACE Rev2 Code 50.1

³⁸ NACE Rev2 Code 50.2

³⁹ 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.

⁴⁰ 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

⁴¹ 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

⁴² 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>)

Enablers of Internet services, e.g. e-commerce platforms, Internet payment gateways, social networks, search engines, cloud computing services, application stores, communication services other than those covered by the electronic communications framework. Software developers and hardware manufacturers are excluded.

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

- 1.1. Title of the proposal/initiative
- 1.2. Policy area(s) concerned in the ABM/ABB structure
- 1.3. Nature of the proposal/initiative
- 1.4. Objectives
- 1.5. Grounds for the proposal/initiative
- 1.6. Duration and financial impact
- 1.7. Management method(s) envisaged

2. MANAGEMENT MEASURES

- 2.1. Monitoring and reporting rules
- 2.2. Management and control system
- 2.3. Measures to prevent fraud and irregularities

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

- 3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected
- 3.2. Estimated impact on expenditure
 - 3.2.1. *Summary of estimated impact on expenditure*
 - 3.2.2. *Estimated impact on operational appropriations*
 - 3.2.3. *Estimated impact on appropriations of an administrative nature*
 - 3.2.4. *Compatibility with the current multiannual financial framework*
 - 3.2.5. *Third-party contributions*
- 3.3. Estimated impact on revenue

LEGISLATIVE FINANCIAL STATEMENT

5. FRAMEWORK OF THE PROPOSAL/INITIATIVE

5.1. Title of the proposal/initiative

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.

5.2. Policy area concerned in the ABM/ABB structure⁴³

- 09 – Communications Networks, Content and Technology

5.3. Nature of the proposal/initiative

- The proposal/initiative relates to a **new action**
- The proposal/initiative relates to a **new action following a pilot project/preparatory action**⁴⁴
- The proposal/initiative relates to **the extension of an existing action**
- The proposal/initiative relates to **an action redirected towards a new action**

5.4. Objectives

5.4.1. *The Commission's multiannual strategic objective(s) targeted by the proposal/initiative*

Security and resilience issues are notably addressed under the Trust and Security chapter of the Digital Agenda for Europe, 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 Network and Information Security (NIS) policy.

Security and resilience are also important aspects of the Internal Security Strategy in Action. Chapter 3 "Raise levels of security for citizens and businesses in cyberspace" includes the action "Improve capabilities for dealing with cyber attacks".

The aim of the proposed Directive is to ensure a high common level of network and information security (NIS) across the EU. This will be achieved by requiring the Member States to increase their preparedness and improve their cooperation with each other, and by requiring operators of critical infrastructure and public administrations to adopt appropriate steps to manage security risks and report serious incidents to the national competent authorities.

Lack of NIS can compromise the vital services depending on network and information systems. As a consequence, it can impede the pursuit of economic activities, and generate substantial financial losses to the economy of the Union.

Moreover, as a communication instrument without frontiers, digital information systems and primarily the Internet, are interconnected across Member States and play an essential role in facilitating the cross-border movement of goods, services and people. Given this intrinsic transnational dimension, a disruption in one Member State can affect other Member States and the EU as a whole. The resilience and stability of network and information systems is therefore essential to the completion of the Digital Single Market and the smooth functioning of the Internal Market as a whole. The likelihood and the frequency of incidents and the inability to ensure efficient protection also undermine public trust and confidence in networks and information services: for example, the 2012 Eurobarometer on Cybersecurity found that 38% of EU Internet users have concerns with the safety of on-line payments and have changed their behaviour because of concerns with

⁴³ ABM: Activity-Based Management – ABB: Activity-Based Budgeting.

⁴⁴ As referred to in Article 49(6)(a) or (b) of the Financial Regulation.

security issues: 18% are less likely to buy goods on-line and 15% are less likely to use on-line banking.

5.4.2. *Specific objectives and ABM/ABB activities concerned*

The proposal lays down measures to ensure a high common level of network and information systems security across the Union.

The specific objectives are:

1. To put in place a minimum level of NIS in the Member States and thus increase the overall level of preparedness and response. To this end, the proposal requires the Member States to have in place a minimum level of national capabilities by setting up competent authorities for NIS and Computer Emergency Response Teams (CERT), as well as by adopting a national NIS strategies and national NIS cooperation plans.

2. To improve cooperation on NIS at EU level with a view to counter cross border incidents and threats effectively. To this end, the national competent authorities would be required to cooperate within a network by exchanging information and working together to counter NIS threats and incidents on the basis of the European NIS cooperation plan.

A secure information-sharing infrastructure will be put in place to allow for the exchange of sensitive and confidential information among the competent authorities.

3. To create a culture of risk management and improve the sharing of information between the private and public sectors. To this end, the proposal establishes NIS risk management requirements for market operators and public administrations as well as the obligation to report NIS incidents with a significant impact to the competent authorities.

ABM/ABB activities concerned

The Directive covers entities (companies and organisations, including some SMEs) in a number of sectors (energy, transport, credit institutions and stock exchanges, healthcare and enablers of key Internet services) as well as public administrations. It addresses links with law enforcement and data protection and NIS aspects of external relations.

- 09 – Communications Networks, Content and Technology
- 02 - Enterprise
- 32 - Energy
- 06 - Mobility and Transport
- 17 - Health and consumer protection
- 18 – Home affairs
- 19 – External relations
- 33 - Justice
- 12- Internal market

5.4.3. *Expected result(s) and impact*

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

The protection of EU consumers, business and Governments against NIS incidents, threats and risks would improve considerably.

The obligations placed on the Member States would ensure preparedness both in terms of technical and organisational capabilities; and would contribute to the creation of a climate of mutual trust, which is a precondition for effective cooperation at EU level.

The setting up of mechanism for cooperation at EU level would deliver coherent and coordinated prevention and response to cross-border NIS incidents and risks.

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 to report NIS incidents with a significant impact would enhance the ability to respond to incidents and 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.

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.

For the Member States, the cost of putting in place national NIS capabilities would be negligible for those who are already well equipped; for those starting from scratch estimated costs are 2.5 million EUR for a CERT; 360 000 EUR for the adoption of a national cyber incident contingency/cooperation plan and a national cyber security strategy; 55 555 EUR per Member State per EU-level cyber incident exercise. The cost of participating to the meetings with other competent authorities within the network would be of 6000 EUR per Member State per year.

The cooperation and exchange of information between Member States would be supported by a secure infrastructure. The proposal would have EU budgetary implications only if Member States choose to adapt an existing infrastructure (e.g. sTESTA) and task the Commission to implement the adaptation under the MFF 2014-2020. The related one-off cost is estimated to be 1 250 000 million EUR and would 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 sufficient funds are available under CEF. Alternatively Member States can either share the one-off cost of the adaptation of an existing infrastructure or decide to set up a new infrastructure and bear the costs, which are estimated to be approximately 10 million EUR per year.

For public administrations and key private players, the introduction of requirements to carry out NIS risk management would create total additional costs that would be in the range from 1 to 2 billion EUR. The compliance cost per small and medium enterprise would fall in the range of 2500 and 5000 EUR. The obligation to report NIS incidents with a significant impact would create cost of 125 EUR per NIS incident notification. In those few cases where an investigation could be open by a competent authority the maximum cost for the entity affected would be 25 000 EUR.

As to the economic impact, as a result of the increased level of security financial losses associated with NIS risks and incidents would 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. 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.

Organisations would be better equipped to handle incidents and attacks, resulting in enhanced availability, reliability and quality of their services.

As to the 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. It is also very likely that employment of NIS personnel in the EU would be boosted due to the requirements to conduct NIS risk assessments and adopt appropriate security measures.

For more information, please refer to the Commission Staff Working Paper on the impact assessment accompanying this legislative proposal.

5.4.4. *Indicators of results and impact*

Specify the indicators for monitoring implementation of the proposal/initiative.

As part of the assessment of the implementation of this Directive, the Commission will verify: (i) that the Member States increase their overall level of preparedness through capacity building and planning; and (ii) the implementation of the NIS risk management and reporting requirements placed on public administrations and key private players.

The setting up and functioning of the cooperation among competent authorities via the network and the adoption of the relevant implementing and delegated acts would indicate Member State and private sector progress in attaining the objectives.

Overall, the following indicators will be of particular importance:

- the requirements to be met at the national level in the short or long term as detailed in Section 1.5.1,
- the level of capabilities and maturity of the NIS market in the Member States,
- the effective functioning of the cooperation via the network.

The Commission would periodically review the functioning of the Directive and report to the European Parliament and the Council. The functioning of the cooperation via the network and the specific objectives under 1.5.1 will constitute key monitoring criteria.

5.5. **Grounds for the proposal/initiative**

5.5.1. *Requirements to be met in the short or long term*

Each Member State would be required to have:

- a national NIS strategy defining the strategic objectives and concrete policy actions to be implemented;
- a NIS cooperation plan;
- a body responsible for coordinating NIS issues (a competent authority) and acting as a focal point for cross-border and cooperation at Union level; and
- a Computer Emergency Response Team (CERT)

At EU level, the Member States would be required to cooperate via a network. A secure information-sharing structure should be put in place to allow for the exchange of sensitive and confidential information. The Commission would be required to adopt by means of implementing acts a plan (European NIS cooperation plan) setting out the modalities and the operational rules of the cooperation network.

Public administrations and key private players would be required to carry out NIS risk management and to report to the competent authorities NIS incidents with a significant impact.

5.5.2. *Added value of EU involvement*

Considering the cross-border nature of NIS, divergences in relevant legislation and policy represent a barrier for companies to operate in multiple countries and to the achievement of global economies of scale. Lack of intervention at EU level would lead to a situation where each Member State would act alone disregarding the interdependences amongst network and information systems. Action at EU level would ensure that an appropriate degree of coordination takes place among the Member States so that governments NIS measures are consistent with each other, and NIS risks are well managed in the cross-border context in which they arise.

The stated objectives can hence be better achieved via EU level action, rather than by the Member States alone.

5.5.3. *Lessons learned from similar experiences in the past*

The proposal stems from the analysis that regulatory obligations are needed to create a level playing field and close some legislative loopholes. In this field, 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 involving all the Member States it is necessary to make sure that all of them have the required minimum level of capabilities.

For more information, please refer to the Commission Staff Working Paper on the impact assessment accompanying this legislative proposal.

5.5.4. *Compatibility and possible synergy with other appropriate instruments*

The proposal is fully consistent with the Trust and Security chapter of the Digital Agenda for Europe and therefore with the EU2020 Strategy. As indicated above, key action 6 of the Digital Agenda for Europe calls for measures aimed at a reinforced and high level NIS policy. It is also consistent with and complements the EU electronic communications regulatory framework, the EU Directive on European Critical Infrastructure and the EU data protection Directive.

The proposal accompanies and is an essential part of the Communication of the Commission and the High Representative of the Union for Foreign Affairs and Security Policy on the European Cybersecurity Strategy.

5.6. Duration and financial impact

- Proposal/initiative of limited duration
- Proposal/initiative in effect from [DD/MM]YYYY to [DD/MM]YYYY
- Financial impact from YYYY to YYYY
- Proposal/initiative of unlimited duration
- Transposition period will start immediately after adoption (estimated in 2015) and run for 18 months. Implementation of the Directive will, however, start after adoption and will entail setting up the secure infrastructure that will support Member State cooperation.
- followed by full-scale operation.

5.7. Management modes envisaged⁴⁵

- Centralised direct management by the Commission
- Centralised indirect management with the delegation of implementation tasks to:
 - executive agencies
 - bodies set up by the Communities⁴⁶
 - national public-sector bodies/bodies with public-service mission
 - persons entrusted with the implementation of specific actions pursuant to Title V of the Treaty on European Union and identified in the relevant basic act within the meaning of Article 49 of the Financial Regulation
 - Shared management with the Member States
 - Decentralised management with third countries
 - Joint management with international organisations, including the European Space Agency

If more than one management mode is indicated, please provide details in the "Comments" section.

Comments:

The cooperation and exchange of information between Member States would be supported by a secure infrastructure. The proposal would have EU budgetary implications only if Member States choose to adapt an existing infrastructure (e.g. sTESTA) and task the Commission to implement the adaptation of it under the MFF 2014-2020. The related one-off cost is estimated to be 1 250 000 million EUR and would 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 sufficient funds are available under CEF. Alternatively Member States can either share the one-off cost of the adaptation of an existing infrastructure or decide to set up a new infrastructure and bear the costs, which are estimated to be approximately 10 million EUR per year.

ENISA, a decentralised Agency created by the Communities, may assist the Member States and the Commission in the implementation of the Directive on the basis of its

⁴⁵ Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.htmlhttp://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

⁴⁶ As referred to in Article 185 of the Financial Regulation.

mandate and by the redeployment of resources foreseen under the MFF 2014-2020 for this agency.

6. MANAGEMENT MEASURES

6.1. Monitoring and reporting rules

Specify frequency and conditions.

The Commission will periodically review the functioning of the Directive and report to the European Parliament and the Council. The first report will be submitted no later than three years after the transposition date, and subsequent reports will be submitted every three years thereafter. The Commission may request information from the Member States, and Member States have the obligation to supply them without undue delay.

The Commission will also assess the correct transposition of the Directive by the Member States.

The CEF proposal also provides for the possibility to undertake an evaluation of the methods of carrying out projects as well as the impact of their implementation, in order to assess whether the objectives, including those relating to environmental protection, have been attained.

On the level of the actions, beneficiaries will provide on a regular basis and on the terms of the agreements/decisions reports on the actions to be implemented. The CEF regulation provides furthermore for the possibility to request Member States specific evaluations of actions and linked projects

6.2. Management and control system

6.2.1. Risk identified

- project implementation delays in building the secure infrastructure

6.2.2. Control methods envisaged

The CEF will mainly be implemented through centralized direct and indirect management by the Commission. Cases of joint management might be envisaged. As regards grants the main elements of the internal control system are the procedures for selection and evaluation of grant proposals (ex-ante controls), technical and financial transaction controls during the management of the projects based on reporting and ex-post audits of beneficiaries. The agreements and decisions for implementing the actions under CEF will provide for supervision and financial control by the Commission, or any representative authorised by the Commission, as well as audits by the Court of Auditors and on-the-spot checks carried out by the European Anti-Fraud Office (OLAF).

6.2.3. Costs and benefits of controls and probable non-compliance rate

Risk based ex-ante and ex-post controls and the possibility of on-site audits will ensure that the costs of the controls are reasonable.

6.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures.

The Commission shall take appropriate measures ensuring that when the action financed under this Directive is implemented, the financial interests of the Union are protected by the application of preventive measures against fraud, corruption and any other illegal activities by effective checks and, if irregularities are detected, by the

recovery of the amounts wrongly paid and, where appropriate, by effective, proportionate and deterrent penalties.

The Commission or its representatives and the Court of Auditors shall have the power of audit, on the basis of documents and on-the-spot, over all grant beneficiaries, contractors and subcontractors who have received Union funds under the Programme.

The European Anti-fraud Office (OLAF) may carry out on-the-spot checks and inspections on economic operators concerned directly or indirectly by such funding in accordance with the procedures laid down in Regulation (Euratom, EC) No 2185/96 with a view to establishing whether there has been fraud, corruption or any other illegal activity affecting the financial interests of the Union in connection with a grant agreement or grant decision or a contract concerning Union funding.

Without prejudice to the paragraphs above, cooperation agreements with third countries and international organisations and grant agreements and grant decisions and contracts resulting from the implementation of this Regulation shall expressly empower the Commission, the Court of Auditors and OLAF to conduct such audits, on-the-spot checks and inspections.

The CEF provides for contracts for grants and procurement to be based on standard models, which will set out the generally applicable anti-fraud measures.

7. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

The estimated financial impact of the proposal will incur if the Member States choose to adapt an existing infrastructure and task the Commission to implement the adaptation of it under the MFF 2014-2020. The related costs would be covered under CEF on condition that sufficient funds are available. Alternatively Member States can either share the costs of the adaptation of the infrastructure or the costs of the setting up of a new infrastructure.

7.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

- Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number [Description.....]	Diff./non-diff. (⁴⁷)	from EFTA countries ⁴⁸	from candidate countries ⁴⁹	from third countries	within the meaning of Article 18(1)(aa) of the Financial Regulation
	09 03 02 To promote the interconnection and interoperability of national public services on-line as well as access to such networks	Diff.	NO	NO	NO	NO

- New budget lines requested (Not applicable)

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number [Heading.....]	Diff./non-diff.	from EFTA countries	from candidate countries	from third countries	within the meaning of Article 18(1)(aa) of the Financial Regulation
	[XX.YY.YY.YY]		YES/N O	YES/N O	YES/N O	YES/NO

⁴⁷ Diff. = Differentiated appropriations / Non-Diff. = Non-differentiated appropriations.

⁴⁸ EFTA: European Free Trade Association.

⁴⁹ Candidate countries and, where applicable, potential candidate countries from the Western Balkans.

7.2. Estimated impact on expenditure

7.2.1. Summary of estimated impact on expenditure

EUR million (to three decimal places)

Heading of multiannual financial framework:	1	Smart and inclusive Growth
--	---	----------------------------

DG: <.....>			2015* 50	Year 2016	Year 2017	Year 2018	Subsequent years (2019-2021)			TOTAL
• Operational appropriations										
09 03 02	Commitments	(1)	1,250**	0,000						1,250
	Payments	(2)	0,750	0,250	0,250					1,250
Appropriations of an administrative nature financed from the envelope of specific programmes ⁵¹			0,000							0,000
Number of budget line		(3)	0,000							0,000
TOTAL appropriations for DG <.....>	Commitments	=1+1a +3	1,250	0,000						1,250
	Payments	=2+2a +3	0,750	0,250	0,250					1,250

• TOTAL operational appropriations	Commitments	(4)	1,250	0,000						1,250
	Payments	(5)	0,750	0,250	0,250					

⁵⁰ Year N is the year in which implementation of the proposal/initiative starts.

⁵¹ Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

• TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)	0,000							
TOTAL appropriations under HEADING 1 of the multiannual financial framework	Commitments	=4+ 6	1,250	0,000						1,250
	Payments	=5+ 6	0,750	0,250	0,250					1,250

* The exact timing will depend on the date of adoption of the proposal by the Legislative Authority (i.e., if the Directive will be approved in the course of 2014, the adaptation of an existing infrastructure would start in 2015, otherwise one year later).

** If Member States choose to use an existing infrastructure and to cover the one-off adaptation cost under the EU budget, as explained under 1.4.3 and 1.7, the cost for the customisation of a network to support cooperation between Member States, according to Chapter III of the Directive (early warning, coordinated response etc.) is estimated to be 1 250 000 EUR. This is based on an estimation of the JRC, based on its experience in developing similar systems for other areas like public health: a Rapid Alerting and Notification System for NIS (€275 000); an Information Exchange Platform (€400 000); an Early Warning and Response System (€275 000); a Situation Room (€300 000) for a total of €1 250 000. A more detailed implementation plan is expected in the forthcoming feasibility study under specific contract SMART 2012/0010: 'Feasibility study and preparatory activities for the implementation of a European early warning and response system against cyber-attacks and disruptions'.

If more than one heading is affected by the proposal / initiative:

• TOTAL operational appropriations	Commitments	(4)	0,000	0,000						
	Payments	(5)	0,000	0,000						
• TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)	0,000	0,000						
TOTAL appropriations under HEADINGS 1 to 4 of the multiannual financial framework (Reference amount)	Commitments	=4+ 6	1,250	0,000						1,250
	Payments	=5+ 6	0,750	0,250	0,250					1,250

Heading of multiannual financial framework	5	'Administrative expenditure'
---	----------	------------------------------

EUR million (to three decimal places)

		Year 2015	Year 2016	Year 2017	Year 2018	Subsequent years (2019-2021)			TOTAL
DG:CNECT									
• Human resources		0,572	0,572	0,572	0,572	0,572	0,572	0,572	4,004
• Other administrative expenditure		0,318	0,118	0,318	0,118	0,318	0,118	0,118	1,426
TOTAL DG CNECT	Appropriations	0,890	0,690	0,890	0,690	0,890	0,690	0,690	5,430

TOTAL appropriations for HEADING 5 of the multiannual financial framework	(Total commitments = Total payments)	0,890	0,690	0,890	0,690	0,890	0,690	0,690	5,430
--	--------------------------------------	-------	-------	-------	-------	-------	-------	-------	--------------

EUR million (to three decimal places)

		Year 2015 ⁵²	Year 2016	Year 2017	Year 2018	Subsequent years (2019-2021)			TOTAL
TOTAL appropriations under HEADINGS 1 to 5 of the multiannual financial framework	Commitments	2,140	0,690	0,890	0,690	0,890	0,690	0,690	6,680
	Payments	1,640	0,940	1,140	0,690	0,890	0,690	0,690	6,680

⁵² Year N is the year in which implementation of the proposal/initiative starts.

7.2.2. *Estimated impact on operational appropriations*

- The proposal/initiative does not require the use of operational appropriations
- The proposal/initiative requires the use of operational appropriations, as explained below:

– Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs ↓			Year 2015*	Year 2016	Year 2017	Year 2018	Subsequent years (2019-2021)						TOTAL						
	OUTPUTS																		
	Type ⁵³	Average cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Total number	Total cost	
SPECIFIC OBJECTIVE NO 2 ⁵⁴ Secure information sharing infrastructure																			
- Output	Adapt infrastructure																		
Subtotal for specific objective No 2			1	1,250													1	1,250	
TOTAL COST				1,250														1,250	

⁵³ Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

⁵⁴ As described in point 1.4.2. ‘Specific objective(s)...’

* The exact timing will depend on the date of adoption of the proposal by the Legislative Authority (i.e., if the Directive will be approved in the course of 2014, the adaptation of an existing infrastructure would start in 2015, otherwise one year later).

The estimated financial impact of the proposal will incur if the Member States choose to adapt an existing infrastructure and task the Commission to implement the adaptation of it under the MFF 2014-2020. The related costs would be covered under CEF on condition that sufficient funds are available. Alternatively Member States can either share the costs of the adaptation of the infrastructure or the costs of the setting up of a new infrastructure.

7.2.3. Estimated impact on appropriations of an administrative nature

7.2.3.1. Summary

- The proposal/initiative does not require the use of administrative appropriations
- The proposal/initiative requires the use of administrative appropriations, as explained below:

EUR million (to three decimal places)

	Year 2015 ⁵⁵	Year 2016	Year 2017	Year 2018	Subsequent years (2019-2021)			TOTAL
--	-------------------------	-----------	-----------	-----------	------------------------------	--	--	-------

HEADING 5 of the multiannual financial framework								
Human resources	0,572	0,572	0,572	0,572	0,572	0,572	0,572	4,004
Other administrative expenditure	0,318	0,118	0,318	0,118	0,318	0,118	0,118	1,426
Subtotal HEADING 5 of the multiannual financial framework	0,890	0,690	0,890	0,690	0,890	0,690	0,690	5,430

Outside HEADING 5⁵⁶ of the multiannual financial framework								
Human resources	0,000	0,000						0,000
Other expenditure of an administrative nature								
Subtotal outside HEADING 5 of the multiannual financial framework	0,890	0,690	0,890	0,690	0,890	0,690	0,690	5,430

⁵⁵ Year N is the year in which implementation of the proposal/initiative starts.

⁵⁶ Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

TOTAL	0,890	0,690	0,890	0,690	0,890	0,690	0,690	5,430
--------------	-------	-------	-------	-------	-------	-------	-------	--------------

The administrative appropriations required will be met by the appropriations of the DG CNECT which are already assigned to management of the action and/or which have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

The European Network Security Agency (ENISA) might assist the member States and the Commission in the implementation of the Directive on the basis of its mandate and by redeployment of resources under MFF 2014-2020 for this agency, i.e, without any additional budgetary or human resources allocations.

7.2.3.2. Estimated requirements of human resources

- The proposal/initiative does not require the use of human resources
- The proposal/initiative requires the use of Commission human resources, as explained below:

In principle no additional manpower would be needed. The human resources required will be very limited and will be met by staff from the DG who are already assigned to the management of the action.

Estimate to be expressed in full time equivalent units

		Year 2015	Year 2016	2017	2018
Management plan posts (officials and temporary agents)					
09 01 01 01 (Headquarters and Commission's Representation Offices)		4	4	4	4
XX 01 01 02 (Delegations)					
XX 01 05 01 (Indirect research)					
10 01 05 01 (Direct research)					
• External personnel (in Full Time Equivalent unit: FTE)⁵⁷					
09 01 02 01 (CA, INT, SNE from the "global envelope")		1	1	1	1
XX 01 02 02 (CA, INT, JED, LA and SNE in the delegations)					
XX 01 04 yy ⁵⁸	- at Headquarters				
	- in delegations				
XX 01 05 02 (CA, SNE, INT - Indirect research)					
10 01 05 02 (CA, SNE, INT - Direct research)					
Other budget lines (specify)					
TOTAL		5	5	5	5

XX is the policy area or budget title concerned.

The human resources required will be met by staff from the DG CNECT who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

The European Network Security Agency (ENISA) might assist the member States and the Commission in the implementation of the Directive on the basis of its current mandate and by redeployment of resources under MFF 2014-2020 for this agency, i.e. without any additional budgetary or human resources allocations.

Description of tasks to be carried out:

Officials and temporary staff	- Preparation of delegated acts according to Article 14 (3) - Preparation of implementing acts according to Articles 8, 9 (2), 12, 14 (5), 16
-------------------------------	--

⁵⁷ CA= Contract Agent; LA = Local Agent; SNE = Seconded National Expert; INT = agency staff ('Intérimaire'); JED= 'Jeune Expert en Délégation' (Young Experts in Delegations).

⁵⁸ Sub-ceiling for external staff covered by operational appropriations (former "BA" lines).

	<ul style="list-style-type: none">- Contribute to cooperation via the network both at policy and operational level.- Engage in international talks and possibly conclusion of international agreements
External staff	Support to all above tasks as necessary.

7.2.4. *Compatibility with the current multiannual financial framework*

- Proposal/initiative is compatible the current multiannual financial framework.
- Proposal/initiative will entail reprogramming of the relevant heading in the multiannual financial framework.

The estimated financial impact of the proposal will incur if the Member States choose to adapt an existing infrastructure and task the Commission to implement the adaptation of it under the MFF 2014-2020. The related costs would be covered under CEF on condition that sufficient funds are available. Alternatively Member States can either share the costs of the adaptation of the infrastructure or the costs of the setting up of a new infrastructure.

- Proposal/initiative requires application of the flexibility instrument or revision of the multiannual financial framework⁵⁹.

Not applicable

7.2.5. *Third-party contributions*

- The proposal/initiative does not provide for co-financing by third parties.

7.3. **Estimated impact on revenue**

- Proposal/initiative has no financial impact on revenue.

⁵⁹ See points 19 and 24 of the Interinstitutional Agreement.

ANNEX to the LEGISLATIVE FINANCIAL STATEMENT

Title of the proposal/initiative:

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.

3. NUMBER and COST of HUMAN RESOURCES CONSIDERED NECESSARY
4. COST of OTHER EXPENDITURE of an ADMINISTRATIVE NATURE
5. METHODS of CALCULATION USED for ESTIMATING COST
 - Human resources
 - Other expenditure of an administrative nature

This annex must accompany the legislative financial statement when the interdepartmental consultation is launched.

The data tables are used as a source for the tables contained in the legislative financial statement. They are strictly for internal use within the Commission.

8. COST OF HUMAN RESOURCES CONSIDERED NECESSARY

- The proposal/initiative does not require the use of human resources
 The proposal/initiative requires the use of human resources, as described below:

EUR million (to 3 decimal places)

HEADING 5 of the multiannual financial framework		Year 2015		Year 2016		Year 2017		Year 2018		Subsequent years (2019-2021)		TOTAL	
		FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations
• Establishment plan posts (officials and temporary staff)													
09 01 01 01 (Headquarters and Commission Representation Offices)	AD	3	0.381	3	0.381	3	0.381	3	0.381	3	0.381		2,667
	AST	1	0.127	1	0.127	1	0.127	1	0.127	1	0.127		0.889
XX 01 01 02 (Headquarters and Commission Representation Offices)	AD												
	AST												
• External staff⁶⁰													
09 01 02 01 (“global envelope”)	CA	1	0.064	1	0.064	1	0.064	1	0.064	1	0.064		0.448
	SNE												
	INT												
XX 01 02 02 (Delegations)	CA												
	LA												
	SNE												

⁶⁰ CA= Contract Agent; INT= agency staff (“Intérimaire”); JED= “Jeune Expert en Délégation” (young experts in Delegations); LA= Local Agent; SNE= Seconded National Expert.

	INT												
	JED												
Other budget lines (<i>please specify</i>)													
Sub-total – HEADING 5 of the multiannual financial framework		5	0.572	5	0.572	5	0.572	5	0.572	5	0.572	5	4,004

XX is the policy area or budget title concerned

The human resources required will be met by staff from DG CNECT who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

The European Network and Information Security Agency (ENISA) might assist the Member States and the Commission in the implementation of the Directive on the basis of its mandate and by redeployment of resources foreseen under the MFF 2014-2020 for this agency (, i.e., without any additional budgetary or human resources allocations).

EUR million (to 3 decimal places)

Outside HEADING 5 of the multiannual financial framework		Year N		Year N+1		Year N+2		Year N+3		... enter as many years as necessary to show the duration of the impact (see point 1.6)		TOTAL	
		FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations
• Establishment plan posts (officials and temporary agents)													
XX 01 05 01 (Indirect research)	AD												
	AST												
10 01 05 01 (Direct research)	AD												
	AST												
• External staff⁶¹													
XX 01 04 yy Sub-ceiling for external staff covered by operational appropriations (former "BA" lines)	Headquarters	CA											
		SNE											
		INT											
	Delegations	CA											
		LA											
		SNE											
		INT											

⁶¹ CA= Contract Agent; INT= agency staff ("Intérimaire"); JED= "Jeune Expert en Délégation" (young experts in Delegations); LA= Local Agent; SNE= Seconded National Expert;

		JED												
XX 01 05 02 (Indirect research)		CA												
		SNE												
		INT												
10 01 05 02 (Direct research)		CA												
		SNE												
		INT												
Other budget lines (<i>please specify</i>)														
Sub-total – Outside HEADING 5 of the multiannual financial framework														
TOTAL			0	0,000									0	0,000

XX is the policy area or budget title concerned

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

9. COST OF OTHER EXPENDITURE OF AN ADMINISTRATIVE NATURE

- The proposal/initiative does not require the use of any appropriation of an administrative nature
 The proposal/initiative requires the use of appropriations of an administrative nature, described as follows:

EUR million (to 3 decimal places)

	Year 2015	Year 2016	Year 2017	Year 2018	Subsequent years (2019-2021)			TOTAL
HEADING 5 of the multiannual financial framework								
Headquarters:								
09 01 02 11 01 - Mission and representation expenses	0.010	0.010	0.010	0.010	0.010	0.010	0.010	0.070
09 01 02 11 02 - Meetings of the network of competent authorities	0.054	0.054	0.054	0.054	0.054	0.054	0.054	0.378
09 01 02 11 03 – Network and Information Security Committee ⁶²	0.054	0.054	0.054	0.054	0.054	0.054	0.054	0.378
09 01 02 11 04 - Studies and consultations	0.200		0.200		0.200			0.600
XX 01 03 01 03 - Equipment and furniture								
XX 01 03 01 04 - +								
Other budget lines (<i>please specify</i>)								
Delegations:								
XX 01 02 12 01 - Missions, conferences and representation expenses								
XX 01 02 12 02 - Further training of staff								

⁶²

A Network and Information Security Committee, within the meaning of Regulation (EU) N182/2011, will be established under the Directive.

XX 01 03 02 01 - Acquisition, renting and related expenditure								
XX 01 03 02 02 - Equipment, furniture, supplies and services								
Sub-total HEADING 5 of the multiannual financial framework	0.318	0.118	0.318	0.118	0.318	0.118	0.118	1,426

XX is the policy area or budget title concerned

EUR million (to 3 decimal places)

	Year N	Year N+1	Year N+2	Year N+3	... enter as many years as necessary to show the duration of the impact (see point 1.6)	TOTAL
--	-----------	-------------	-------------	-------------	---	-------

Outside HEADING 5 of the multiannual financial framework								
XX 01 04 yy - Expenditure on technical and administrative assistance (<u>not including</u> external staff) from operational appropriations (former "BA" lines)								
- Headquarters								
- Delegations								
XX 01 05 03 – Other management expenditure for indirect research								
10 01 05 03 - Other management expenditure for direct research								
Other budget lines (<i>please specify</i>)								
Sub-total Outside HEADING 5 of the multiannual financial framework	0,000							0,000

XX is the policy area or budget title concerned

TOTAL HEADING 5 and Outside HEADING 5 of the multiannual financial framework	0,890	0,690	0,890	0,690	0,890	0,690	0,690	5,430
--	-------	-------	-------	-------	-------	-------	-------	--------------

The administrative appropriations required will be met by the appropriations which are already assigned to management of the action and/or which have been redeployed, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

10. METHODS OF CALCULATION USED TO ESTIMATE COSTS

10.1. Human resources

This part will set out the method of calculation used to estimate the human resources considered necessary (workload assumptions, including specific jobs (Sysper 2 work profiles), staff categories and the corresponding average costs)

HEADING 5 of the multiannual financial framework
NB: The average costs for each category of staff at Headquarters are available on BudgWeb at the following site: http://www.cc.cec/budg/pre/legalbasis/pre-040-020_preparation_en.html#forms
<ul style="list-style-type: none">• Officials and temporary staff <p>It has been calculated that 4 people already working on this issue (3 AD and 1 AST) will continue to do so in the future, thus 4 x 127.000€/year (=508.000€/year).</p>
<ul style="list-style-type: none">• External staff <p>It has been calculated that 1 person already working on this issue (1CA) will continue to do so in the future, thus 1x 64.000€/year.</p>

Outside HEADING 5 of the multiannual financial framework (where applicable)
<ul style="list-style-type: none">• Only posts financed from the research budget
<ul style="list-style-type: none">• External staff

10.2. Other expenditure of an administrative nature

Give details of the method of calculation used for each budget line

and, in particular, the underlying assumptions (e.g. number of meetings per year, average costs, etc.)

HEADING 5 of the multiannual financial framework
<p>For missions an average number of 4 missions per year at cost of €500/person has been assumed. For meetings of the network of competent national authorities 4 meetings per year has been assumed, with one representatives per Member State at an average cost of €500/person. For meetings of the Network and Information Security Committee, instituted by the Directive, 4 meetings per year has been assumed, with one representatives per Member State at an average cost of €500/person. One study every two years is foreseen, in preparation of the various implementing measures, at a cost of €200,000/study.</p>

Outside HEADING 5 of the multiannual financial framework

