EUROPEAN
COMMISSION

Brussels, 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

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(2013) 31 final}
{SWD(2013) 32 final}

EXPLANATORY MEMORANDUM

The aim of the proposed Directive is to ensure a high common level of network and information security (NIS). This means improving the security of the Internet and the private networks and information systems underpinning the functioning of our societies and economies. 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 infrastructures, such as energy, transport, and key providers of information society services (e-commerce platforms, social networks, etc), as well as public administrations to adopt appropriate steps to manage security risks and report serious incidents to the national competent authorities.

This proposal is presented in connection with the joint Communication of the Commission and High Representative of the Union for Foreign Affairs and Security Policy on a European Cybersecurity Strategy. 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 under the Strategy in this area focus on raising awareness, developing an internal market for cybersecurity products and services, and fostering R&D investment. These actions will be complemented by others aimed at stepping up the fight against cybercrime and 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. NIS is also an important precondition to create a reliable environment for worldwide trade in services. However, information systems can 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 vital services depending on the integrity of network and information systems. This can stop businesses functioning, generate substantial financial losses for the EU economy and negatively affect societal welfare.

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

Moreover, as a borderless communication instrument, digital information systems, in particular 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. The likelihood and 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 are concerned about the safety of online payments and have changed their behaviour because of concerns with security issues: 18% are less likely to buy goods online and 15% are less likely to use online banking[2].

The current situation in the EU, reflecting the purely voluntary approach followed so far, does not provide sufficient protection against NIS incidents and risks across the EU. Existing NIS capabilities and mechanisms are simply insufficient to keep pace with the fast-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 EU. Given the fact that networks and systems are interconnected, the overall NIS of the EU is weakened by those Member States with an insufficient level of protection. This situation also hinders the creation of trust among peers, which is a prerequisite for cooperation and information sharing. As a result, there is cooperation only among 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 among the Member States. This may result in uncoordinated regulatory interventions, incoherent strategies and divergent standards, leading to insufficient protection against NIS across the EU. Internal Market barriers may also arise, generating compliance costs for companies operating in more than one Member State.

[2] Eurobarometer 390/2012.

Finally, the players managing critical infrastructure or providing services essential to the functioning of our societies are not under appropriate obligations to adopt risk management measures and exchange information with relevant authorities. On the one hand, therefore, businesses lack effective incentives to conduct serious risk management, involving risk assessment and taking appropriate steps to ensure NIS. On the other hand, a large proportion of incidents does not reach the competent authorities and go unnoticed. However, information on incidents is essential for public authorities to react, take appropriate mitigating measures, and set adequate strategic priorities for NIS.

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, internet 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 that they have in place a minimum level of national capabilities by establishing competent authorities for NIS, setting up Computer Emergency Response Teams (CERTs), and adopting national NIS strategies and national NIS cooperation plans.

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

Thirdly, based on the model of the Framework Directive for electronic communications, the proposal aims to ensure that a culture of risk management develops and that information is shared between the private and public sectors. Companies in the specific critical sectors outlined above and public administrations will be required to assess the risks they face and adopt appropriate and proportionate measures to ensure NIS. These entities will be required to report to the competent authorities any incidents seriously compromising their networks and information systems and significantly affecting the continuity of critical services and supply of goods.

1.2. General context

Already in 2001, in its Communication Network and Information Security: Proposal for A European Policy Approach', the Commission outlined the increasing importance of NIS[3]. This was followed by the adoption in 2006 of a Strategy for a Secure Information Society[4], aiming to develop a culture of NIS in Europe. Its main elements were endorsed in a Council Resolution[5].

---

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.

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. The Communication launched an action plan to support Member States' efforts to ensure prevention and response. 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 Europe[8] (DAE), adopted in May 2010, and the related Council Conclusions[9] highlighted the shared understanding that trust and security are fundamental pre-conditions for the wide uptake of ICT and thus for achieving the objectives of the 'smart growth' dimension of the Europe 2020 Strategy[10]. 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.

In its Communication on CIIP of March 2011 on 'Achievements and next steps: towards global cyber-security'[11], 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 tackling 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 announced a number of actions, with the Commission calling 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 of 27 May 2011 on CIIP, the Council of the European Union stressed the pressing need to make ICT systems and networks resilient and secure against all possible disruptions, whether accidental or intentional, to develop across the EU a high level of preparedness, security and resilience capabilities, to upgrade technical competences to allow Europe to meet 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)[12], with the aim of contributing to ensuring a high level and developing a culture of NIS within the EU.A proposal to modernise the mandate of ENISA was adopted on 30 September 2010[13] and is under discussion in the Council and the European Parliament. The revised regulatory framework for electronic communications[14], in force since November 2009, imposes security obligations on

6 COM(2009) 149.
7 2009/C 321/01.
8 COM(2010) 245.
9 Council Conclusions of 31 May 2010 on the Digital Agenda for Europe (10130/10).
10 COM(2010) 2020 and Conclusions of the European Council of 25/26 March 2010 (EUCO 7/10).
11 COM(2011) 163.
12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML.
13 COM(2010) 521.
14 See http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

electronic communication providers[15]. These obligations had to be transposed at national level by May 2011.

All players that are data controllers (for example banks or hospitals) are obliged by the data protection regulatory framework[16] to put in place security measures to protect personal data. Also, under the 2012 Commission proposal for a General Data Protection Regulation[17], data controllers would have to report breaches of personal data to the national supervisory authorities. This means that, for example, a NIS security breach affecting the provision of a service without compromising personal data (e.g. an ICT outage at a power company resulting 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)'[18] 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 oblige 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-legislators are currently discussing the Commission proposal for a Directive on attacks against information systems[19], which aims to harmonise the criminalisation of specific types of conduct. It covers only the criminalisation of specific types of conduct and does not address the prevention of NIS risks and incidents, the response to NIS incidents and the mitigation of their impact. The present Directive should apply without prejudice to the Directive on attacks against information systems.

On 28 March 2012, the Commission adopted a Communication on the establishment of a European Cybercrime Centre (EC3)[20]. This Centre, established on 11 January 2013, is 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, in close cooperation with Eurojust, become the collective voice of European cybercrime investigators across law enforcement and the judiciary.

The European Institutions, agencies and bodies have set up their own Computer Emergency Response Team, called CERT-EU.

At international level, the EU works on cybersecurity at both bilateral and multilateral level. The 2010 EU-US Summit[21] saw the establishment of the EU-US Working Group on Cybersecurity and Cybercrime. The EU is also active in other relevant 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).

---

15 Articles 13a and 13b of the Framework Directive.

16 Directive 2002/58 of 12 July 2002.

17 COM(2012) 11.

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

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

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

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

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 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 information and systems were unaware of existing NIS threats and incidents; 66.3% would in principle be in favour of introducing 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 thought that it would be important to adopt NIS requirements in the following sectors in particular: banking and finance (91.1%), energy (89.4%), transport (81.7%), health (89.4%), internet services (89.1%), and public administrations (87.5%). Respondents also considered 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 public administrations should also be subject to it (93.5%). Finally, respondents affirmed that a requirement to implement NIS risk management in line with the state of the art would entail for them no significant additional costs (63.4%), and that a requirement to report security breaches would cause no significant additional costs (72.3%).

Member States were consulted in a number of relevant Council configurations, in the context of the European Forum for Member States (EFMS), at 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 were also held within the European Public-Private Partnership for Resilience[22] and through bilateral meetings. As for the public sector, the Commission held discussions with ENISA and the CERT for the EU institutions.

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 for NIS regarding Member State capabilities, mechanisms for EU-level cooperation, and requirements for key private players and public administrations;

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

The Commission concluded that Option 2 would have the strongest positive impacts, as it would considerably improve the protection of EU consumers, business and governments against NIS incidents. 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 implement NIS risk management for public administrations and key

[22] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

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 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 on Member States. The costs for the private sector would also be limited since many of the entities concerned are already supposed to comply with existing security requirements (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.

This proposal observes the principles recognised by the Charter of Fundamental Rights of the European Union notably, the right to respect for private life and communications. the protection for personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive must be implemented according to these rights and principles.

3. LEGAL ELEMENTS OF THE PROPOSAL

3.1. Legal basis

The European 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 of the Treaty on the Functioning of the European Union — TFEU). Under Article 114 TFEU, the EU 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 is global in 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 establishing ENISA[23], 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 interdependencies among EU network and information systems. An appropriate degree of coordination among

[23] 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).

the Member States would ensure that NIS risks could be well managed in the cross-border context in which they arise. Divergences in NIS regulations represent a barrier to companies wanting to operate in several countries and to the achievement of global economies of scale.

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 only among a minority of Member States with a high level of capabilities. In order to involve 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 one other and be coordinated to contain and minimise the consequences of NIS incidents. Within the network, through exchange of best practices and continuous involvement of ENISA, the competent authorities and the Commission will cooperate to facilitate a convergent implementation of the Directive across the EU. In addition, concerted NIS policy actions can have a strong positive impact for 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 of existing national policies and facilitate their development.

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. This also enables Member States to take due account of national specificities and ensures that the common EU principles are applied in a proportionate manner. The wide scope of application will allow the Member States to implement the Directive in light of the actual risks faced at national level as identified in the national NIS strategy. The requirements to implement 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.

To avoid imposing a disproportionate burden on small operators, in particular on SMEs, the requirements are proportionate to the risk presented by the network or information system concerned and should not apply to micro enterprises. The risks will have to be identified in the first place by the entities subject to these obligations, which will have to decide on the measures to be adopted to mitigate such risks.

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, the proposed Directive does not go beyond what is necessary in order to achieve those objectives.

To achieve 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. The Commission's proposal also strives to support a process of proportionality in the implementation of the obligations placed upon private and public operators.

In order to ensure 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.

Considering in particular the broad scope of the proposed Directive, the fact that it tackles heavily regulated domains, and the legal obligations deriving from its Chapter IV, Explanatory Documents should accompany the notification of transposition measures. In accordance with the Joint Political Declaration of Member States and the Commission on explanatory documents of 28 September 2011, Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a Directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

4. BUDGETARY IMPLICATIONS

Cooperation and exchange of information between Member States should be supported by a secure infrastructure. The proposal will have EU budgetary implications only if Member States choose to adapt an existing infrastructure (e.g. sTESTA) and task the Commission to implement this under the MFF 2014-2020. The one-off cost is estimated to be EUR 1 250 000 and would be borne by the EU budget, budget line 09.03.02 (to promote the interconnection and interoperability of national public services online 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 adapting an existing infrastructure or decide to set up a new infrastructure and bear the costs, which are estimated to be approximately EUR 10 million per year.

2013/0027 (COD)

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,

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

Having regard to the opinion of the European Economic and Social Committee[1],

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 the society. Their reliability and security are essential to economic activities and social welfare, and in particular to 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 that transnational nature, substantial disruption of those systems in one Member State can also affect other Member States and the Union 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 that mechanism to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of NIS 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.

[1] OJ C […], […], p. […].

(5) To cover all relevant incidents and risks, this Directive should apply to all network and information systems. The obligations on public administrations and market operators should however not apply to undertakings providing public communication networks or publicly available electronic communication services within the meaning 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 (Framework Directive)[2], which are subject to the specific security and integrity requirements laid down in Article 13a of that Directive nor should they apply to trust service providers.

(6) The existing capabilities are not sufficient enough 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 NIS within the Union. Lack of common minimum requirements on public administrations 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 challlenges of the security of network and information systems therefore requires a global 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 should be 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 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 the provisions adopted pursuant to this Directive, a body responsible for coordinating NIS 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 to and mitigate network and information systems' 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 deal with incidents and risks and ensure efficient cooperation at Union level.

[2] OJ L 108, 24.4.2002, p. 33.

(12) Building upon the significant progress within the European Forum of Member States ("EFMS") in fostering discussions and exchanges on good policy practices including the development of principles for European cyber crisis cooperation, 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. In particular, in the application of this Directive, the Commission should consult ENISA. To ensure effective and timely information to the Member States and the Commission, early warnings on incidents and risks should be notified within the cooperation network. To build capacity and knowledge among Member States, the cooperation 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.

(14) A secure information-sharing infrastructure should be put in place to allow for the exchange of sensitive and confidential information within the cooperation network. Without prejudice to their obligation to notify incidents and risks of Union dimension to the cooperation network, access to confidential information from other Member States should only be granted to Members 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.

(15) As most network and information systems are privately operated, cooperation between the public and private sector is essential. Market operators should be encouraged to pursue their own informal cooperation mechanisms to ensure NIS. They should also cooperate with the public sector and share information and best practices in exchange of operational support in case of incidents.

(16) To ensure transparency and properly inform EU citizens and market operators, the competent authorities should set up a common website to publish non confidential information on the incidents and risks.

(17) 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.

(18) On the basis in particular of national crisis management experiences and in cooperation with ENISA, the Commission and the Member States should develop a Union NIS cooperation plan defining cooperation mechanisms to counter risks and incidents. That plan should be duly taken into account in the operation of early warnings within the cooperation network.

(19) 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 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 cooperation network.

(20) Upon receipt of an early warning and its assessment, the competent authorities should agree on a coordinated response under the Union NIS cooperation plan. Competent authorities as well as the Commission should be informed about the measures adopted at national level as a result of the coordinated response.

(21) Given the global nature of NIS problems, there is a need for closer international cooperation to improve security standards and information exchange, and promote a common global approach to NIS issues.

(22) Responsibilities in ensuring NIS 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 to the effective functioning of the cooperation network to ensure effective cooperation from all Member States.

(23) Directive 2002/21/EC requires that undertakings providing 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 requirements. 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)[3] 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) Those obligations should be extended beyond the electronic communications sector to key providers of information society services, as defined in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services[4], which underpin downstream information society services or on-line activities, such as e-commerce platforms, Internet payment gateways, social networks, search engines, cloud computing services, application stores. Disruption of these enabling information society services prevents the provision of other information society services which rely on them as key inputs. Software developers and hardware manufacturers are not providers of information society services and are therefore excluded. Those obligations should also be extended to public administrations, and operators of critical infrastructure which rely heavily on information and communications technology and are essential to the maintenance of vital economical or societal functions such as electricity and gas, transport, credit institutions, stock exchange and health. Disruption of those network and information systems would affect the internal market.

(25) Technical and organisational measures imposed to public administrations and market operators should not require that a particular commercial information and communications technology product be designed, developed or manufactured in a particular manner.

(26) The public administrations and market operators should ensure security of the networks and systems which are under their control. These would be primarily private networks and systems managed either by their internal IT staff or the security of which

[3] OJ L 201, 31.7.2002, p. 37.
[4] OJ L 204, 21.7.1998, p. 37.

has been outsourced. The security and notification obligations should apply to the relevant market operators and public administrations regardless of whether they perform the maintenance of their network and information systems internally or outsource it.

(27) 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.

(28) Competent authorities should pay due attention to preserving informal and trusted channels of information-sharing between market operators and between the public and the private sectors. Publicity of incidents reported to the competent authorities should duly balance the interest of the public in being informed about threats with possible reputational and commercial damages for the public administrations and market operators reporting incidents. In the implementation of the notification obligations, competent authorities should pay particular attention to the need to maintain information about product vulnerabilities strictly confidential prior to the release of appropriate security fixes.

(29) Competent authorities should have the necessary means to perform their duties, including powers to obtain sufficient information from market operators and public administrations in order to assess the level of security of network and information systems as well as reliable and comprehensive data about actual incidents that have had an impact on the operation of network and information systems.

(30) Criminal activities are in many cases underlying an 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. The serious criminal nature of incidents should be assessed in the light of EU laws on cybercrime.

(31) Personal data are in many cases compromised as a result of incidents. In this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle the personal data breaches resulting from incidents. Member states shall implement the obligation to notify security incidents in a way that minimises the administrative burden in case the security incident is also a personal data breach in line with the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data[5]. Liaising with the competent authorities and the data protection authorities, ENISA could assist by developing information exchange mechanisms and templates avoiding the need for two notification templates. This single notification template would facilitate the reporting of incidents compromising personal data thereby easing the administrative burden on businesses and public administrations.

(32) Standardisation of security requirements is a market-driven process. To ensure a convergent application of security standards, Member States should encourage

[5] SEC(2012) 72 final

compliance or conformity with specified standards to ensure a high level of security at Union level. To this end, it might be necessary to draft harmonised standards, which should be done in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council[6].

(33) 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.

(34) In order to allow for the proper functioning of the cooperation network, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of the definition of the criteria to be fulfilled for a Member State to be authorized to participate to the secure information-sharing system, of the further specification of the triggering events for early warning, and of the definition of the circumstances in which market operators and public administrations are required to notify incidents.

(35) It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

(36) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission as regards the cooperation between competent authorities and the Commission within the cooperation network, the access to the secure information-sharing infrastructure, the Union NIS cooperation plan, the formats and procedures applicable to informing the public about incidents, and the standards and/or technical specifications relevant to NIS. Those 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 powers[7].

(37) In the application of this Directive, the Commission should liaise as appropriate with relevant sectoral committees and relevant bodies set up at EU level in particular in the field of energy, transport and health.

(38) Information that is considered confidential by a competent authority, in accordance with Union and national rules on business confidentiality, should be exchanged with the Commission and other competent authorities only where such exchange is strictly necessary for the application of this Directive. The information exchanged should be limited to that which is relevant and proportionate to the purpose of such exchange.

(39) The sharing of information on risks and incidents within the cooperation network and compliance with the requirements to notify incidents to the national competent authorities may require the processing of personal data. Such a processing of personal

[6] OJ L 316, 14.11.2012, p. 12.
[7] OJ L 55, 28.2.2011, p.13.

data is necessary to meet the objectives of public interest pursued by this Directive and is thus legitimate under Article 7 of Directive 95/46/EC. It does not constitute, in relation to these legitimate aims, a disproportionate and intolerable interference impairing the very substance of the right to the protection of personal data guaranteed by Article 8 of the Charter of fundamental rights. In the application of this Directive, Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents[8] should apply as appropriate. When data are processed by Union institutions and bodies, such processing 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 data.

(40) Since the objectives of this Directive, namely to ensure a high level of NIS in the Union, cannot be sufficiently achieved by the Member States alone and can therefore, by reason of the 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 those objectives.

(41) This Directive respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union notably, the right to respect for private life and communications, the protection for personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive must be implemented according to these rights and principles

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 security (hereinafter referred to as "NIS") within the Union.

2. To that end, this Directive:

(a) lays down obligations for all Member States concerning the prevention, the handling of and the response to risks and incidents affecting networks and information systems;

(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 risks and incidents affecting network and information systems;

(c) establishes security requirements for market operators and public administrations.

[8] OJ L 145, 31.5.2001, p. 43.

3. The security requirements provided for in Article 14 shall apply neither to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC, which shall comply with the specific security and integrity requirements laid down in Articles 13a and 13b of that Directive, nor to trust service providers.

4. This Directive shall be without prejudice to EU laws on cybercrime 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[9]

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 data[10,] 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 and to the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data[11].

6. The sharing of information within the cooperation network under Chapter III and the notifications of NIS incidents under Article 14 may require the processing of personal data. Such processing, which is necessary to meet the objectives of public interest pursued by this Directive, shall be authorised by the Member State pursuant to Article 7 of Directive 95/46/EC and Directive 2002/58/EC, as implemented in national law.

Article 2

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 Union law.

Article 3

Definitions

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

(1) "network and information system" means:

(a) an electronic communications network within the meaning of Directive 2002/21/EC, and

(b) any device or group of inter-connected or related devices, one or more of which, pursuant to a program, perform automatic processing of computer data, as well as

(c) computer data stored, processed, retrieved or transmitted by elements covered under point (a) and (b) for the purposes of their operation, use, protection and maintenance.

---

9 OJ L 345, 23.12.2008, p. 75.
10 OJ L 281 , 23/11/1995 p. 31.
11 SEC(2012) 72 final.

(2) "security" means the ability of a network and information system to resist, at a given level of confidence, accident or malicious action that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system;

(3) "risk" means any circumstance or event having a potential adverse effect on security;

(4) "incident" means any circumstance or event having an actual adverse effect on security;

(5) "information society service" mean service within the meaning of point (2) of Article 1 of Directive 98/34/EC;

(6) "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 a risk or an incident affecting them;

(7) "incident handling" means all procedures supporting the analysis, containment and response to an incident;

(8) "market operator" means:

(a) provider of information society services which enable the provision of other information society services, a non exhaustive list of which is set out in Annex II;

(b) operator 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, a non exhaustive list of which is set out in Annex II.

(9) "standard" means a standard referred to in Regulation (EU) No 1025/2012;

(10) "specification" means a specification referred to in Regulation (EU) No 1025/2012;

(11) "Trust service provider" means a natural or legal person who provides any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals.

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 and national NIS cooperation plan

1. Each Member State shall adopt 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 following issues:

(a) The definition of the objectives and priorities of the strategy based on an up-to-date risk and incident 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) The identification of the general measures on preparedness, response and recovery, including cooperation mechanisms between the public and private sectors;

(d) An indication of the education, awareness raising and training programmes;

(e) Research and development plans and a description of how these plans reflect the identified priorities.

2. The national NIS strategy shall include a national NIS cooperation plan complying at least with the following requirements

(a) A risk assessment plan to identify risks and assess the impacts of potential incidents;

(b) The definition of the roles and responsibilities of the various actors involved in the implementation of the plan;

(c) The 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.

3. The national NIS strategy and the national NIS cooperation plan shall be communicated to the Commission within one month from their adoption.

Article 6

National competent authority on the security of network and information systems

1. Each Member State shall designate a national competent authority on the security of network and information systems (the "competent authority").

2. The competent authorities shall monitor the application of this Directive at national level and contribute to its consistent application throughout the Union.

3. 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.

4. 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.

5. The competent authorities shall consult and cooperate, whenever appropriate, with the relevant law enforcement national authorities and data protection authorities.

6. 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

1. Each Member State shall set up a Computer Emergency Response Team (hereinafter: "CERT") responsible for handling incidents and risks according to a well-defined process, which shall comply with the requirements set out in point (1) of Annex I. A CERT may be established within the competent authority.

2. Member States shall ensure that CERTs have adequate technical, financial and human resources to effectively carry out their tasks set out in point (2) of Annex I.

3. 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 referred to in Article 9.

4. Member States shall inform the Commission about the resources and mandate as well as the incident handling process of the CERTs.

5. 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 ("cooperation network") to cooperate against risks and incidents affecting network and information systems.

2. The cooperation 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 cooperation network by providing its expertise and advice.

3. Within the cooperation network the competent authorities shall:

   (a) circulate early warnings on risks and incidents in accordance with Article 10;

   (b) ensure a coordinated response in accordance with Article 11;

   (c) publish on a regular basis non-confidential information on on-going early warnings and coordinated response on a common website;

   (d) 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.

   (e) 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;

   (f) cooperate and exchange information on all relevant matters with the EuropeanCybercrime Center within Europol, and with other relevant European

bodies in particular in the fields of data protection, energy, transport, banking, stock exchanges and health;

(g) exchange information and best practices between themselves and the Commission, and assist each other in building capacity on NIS;

(h) organise regular peer reviews on capabilities and preparedness;

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

4. The Commission shall establish, by means of implementing acts, 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 consultation procedure referred to in Article 19(2).

Article 9

Secure information-sharing system

1. The exchange of sensitive and confidential information within the cooperation network shall take place through a secure infrastructure.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 18 concerning the definition of the criteria to be fulfilled for a Member State to be authorized to participate to the secure information-sharing system, regarding:

(a) the availability of a secure and resilient communication and information infrastructure at national level, compatible and interoperable with the secure infrastructure of the cooperation network in compliance with Article 7(3), and

(b) the existence of adequate technical, financial and human resources and processes for their competent authority and CERT allowing an effective, efficient and secure participation in the secure information-sharing system under Article 6(3), Article 7(2) and Article 7(3).

3. The Commission shall adopt, by means of implementing acts, decisions on the access of the Member States to this secure infrastructure, pursuant to the criteria referred to in paragraph 2 and 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).

Article 10

Early warnings

1. The competent authorities or the Commission shall provide early warnings within the cooperation 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.

2. 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.

3. 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.

4. 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 European Cybercrime Centre within Europol.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 18, concerning the further specification of the risks and incidents triggering early warning referred to in paragraph 1.

Article 11

Coordinated response

1. Following an early warning referred to in Article 10 the competent authorities shall, after assessing the relevant information, agree on a coordinated response in accordance with the Union NIS cooperation plan referred to in Article 12.

2. The various measures adopted at national level as a result of the coordinated response shall be communicated to the cooperation network.

Article 12

Union NIS cooperation plan

1. The Commission shall be empowered to adopt, by means of implementing acts, a Union NIS cooperation plan. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).

2. The Union NIS cooperation plan shall provide for:

   (a) for the purposes of Article 10:

      – a definition of the format and procedures for the collection and sharing of compatible and comparable information on risks and incidents by the competent authorities,

      – a definition of the procedures and the criteria for the assessment of the risks and incidents by the cooperation network.

   (b) the processes to be followed for the coordinated responses under Article 11, including identification of roles and responsibilities and cooperation procedures;

   (c) a roadmap for NIS exercises and training to reinforce, validate, and test the plan;

   (d) a programme for transfer of knowledge between the Member States in relation to capacity building and peer learning;

   (e) a programme for awareness raising and training between the Member States.

3. The Union NIS cooperation plan 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 cooperation 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 cooperation network. Such agreement shall take into account the need to ensure adequate protection of the personal data circulating on the cooperation 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 incidents affecting their network and information system on the core 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 security of the core services they provide.

3. The requirements under paragraphs 1 and 2 apply to all market operators providing services within the European Union.

4. 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 cooperation network on the notifications received and the action taken in accordance with this paragraph.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 18 concerning the definition of circumstances in which public administrations and market operators are required to notify incidents.

6. Subject to any delegated act adopted under paragraph 5, the competent authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which public administrations and market operators are required to notify incidents.

7. The Commission shall be empowered to define, by means of implementing acts, the formats and procedures applicable for the purpose of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).

8. Paragraphs 1 and 2 shall not apply to microenterprises as defined in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises[12].

[12] OJ L 124, 20.5.2003, p. 36.

Article 15

Implementation and enforcement

1. Member States shall ensure that the competent authorities have all the powers necessary to investigate cases of non-compliance of public administrations or market operators with their obligations under Article 14 and the effects thereof on the security of networks and information systems.

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) undergo a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority.

3. Member States shall ensure that competent authorities have the power to issue binding instructions to market operators and public administrations.

4. The competent authorities shall notify incidents of a suspected serious criminal nature to law enforcement authorities.

5. The competent authorities shall work in close cooperation with personal data protection authorities when addressing incidents resulting in personal data breaches.

6. Member States shall ensure that any obligations imposed on public administrations and market operators under this Chapter may be subject to judicial review.

Article 16

Standardisation

1. To ensure convergent implementation of Article 14(1), Member States shall encourage the use of standards and/or specifications relevant to networks and information security.

2. The Commission shall draw up, by means of implementing acts a list of the standards referred to in paragraph 1. The list shall be published in the Official Journal of the European Union.

CHAPTER V

FINAL PROVISIONS

Article 17

Sanctions

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

2. Member states shall ensure that when a security incident involves personal data, the sanctions foreseen are consistent with the sanctions provided by the Regulation of

the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data[13].

Article 18

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.

2. The power to adopt delegated acts referred to in Articles 9(2), 10(5) and 14(5) 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 Articles 9(2), 10(5) and 14(5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke 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 Articles 9(2), 10(5) and 14(5) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two 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 two months at the initiative of the European Parliament or of the Council.

Article 19

Committee procedure

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 20

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

[13] SEC(2012) 72 final

years after the date of transposition referred to in Article 21. For this purpose, the Commission may request Member States to provide information without undue delay.

Article 21

Transposition

4. Member States shall adopt and publish, by [one year and a half after adoption] at the latest, 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 [one year and a half after adoption].

   When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

5. 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 22

Entry into force

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

Article 23

Addressees

This Directive is addressed to the Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

ANNEX I

Requirements and tasks of the Computer Emergency Response Team (CERT)

The 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) Requirements for the CERT

(a) 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 shall be clearly specified and well known to the constituency and cooperative partners.

(b) The CERT shall implement and manage security measures to ensure the confidentiality, integrity, availability and authenticity of information it receives and treats.

(c) The offices of the CERT and the supporting information systems shall be located in secure sites.

(d) A service management quality system shall be created to follow-up on the performance of the CERT and ensure a steady process of improvement. It shall be based on clearly defined metrics that include formal service levels and key performance indicators.

(e) 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 adequately 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 CERT

(a) Tasks of 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 risks and incidents,
- Responding to incidents,
- Providing dynamic risk and incident analysis and situational awareness,
- Building broad public awareness of the risks associated with online activities,
- Organising campaigns on NIS;

(b) The CERT shall establish cooperative relationships with private sector.

(c) To facilitate cooperation, the CERT shall promote the adoption and use of common or standardised practises for:

- incident and risk handling procedures,
- incident, risk and information classification schemes,

– taxonomies for metrics,

– information exchange formats on risks, incidents, and system naming conventions.

ANNEX II

List of market operators

Referred to in Article 3(8) a):

1. e-commerce platforms
2. Internet payment gateways
3. Social networks
4. Search engines
5. Cloud computing services
6. Application stores

Referred to in Article (3(8) b):

1. Energy
   - Electricity and gas suppliers
   - Electricity and/or gas distribution system operators and retailers for final consumers
   - Natural gas transmission system operators, storage operators and LNG operators
   - Transmission system operators in electricity
   - Oil transmission pipelines and oil storage
   - Electricity and gas market operators
   - Operators of oil and natural gas production, refining and treatment facilities
2. Transport
   - Air carriers (freight and passenger air transport)
   - Maritime carriers (sea and coastal passenger water transport companies and sea and coastal freight water transport companies)
   - Railways (infrastructure managers, integrated companies and railway transport operators)
   - Airports
   - Ports
   - Traffic management control operators
   - Auxiliary logistics services (a) warehousing and storage, b) cargo handling and c) other transportation support activities)
3. Banking: credit institutions in accordance with Article 4.1 of Directive 2006/48/CE.
4. Financial market infrastructures: stock exchanges and central counterparty clearing houses
5. Health sector: health care settings (including hospitals and private clinics) and other entities involved in health care provisions

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

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. 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.

1.2. Policy area concerned in the ABM/ABB structure[37]

- 09 – Communications Networks, Content and Technology

1.3. 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**[38]

☐ The proposal/initiative relates to **the extension of an existing action**

☐ The proposal/initiative relates to **an action redirected towards a new action**

1.4. Objectives

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

The aim of the proposed Directive is to ensure a high common level of network and information security (NIS) across the EU.

1.4.2. 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.

2. To improve cooperation on NIS at EU level with a view to counter cross border incidents and threats effectively. 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.

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

[37] ABM: Activity-Based Management – ABB: Activity-Based Budgeting.

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

- 17 - Health and consumer protection

- 18 – Home affairs

- 19 – External relations

- 33 - Justice

- 12- Internal market

1.4.3. 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.

Further details can be found in Section 8.2 (Impact of Option 2 – Regulatory approach) of the Commission Staff Working Document Impact Assessment accompanying this legislative proposal.

1.4.4. Indicators of results and impact

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

The indicators for Monitoring and Evaluation can be found in Section 10 of the Impact Assessment.

1.5. Grounds for the proposal/initiative

1.5.1. Requirements to be met in the short or long term

Each Member State would be required to have:

- a national NIS strategy;

- a NIS cooperation plan;

- a NIS competent national authority; and

- a Computer Emergency Response Team (CERT)

At EU level, the Member States would be required to cooperate via a 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.

1.5.2. 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.

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

1.5.3. 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.

1.5.4. Compatibility and possible synergy with other appropriate instruments

The proposal is fully consistent with the Digital Agenda for Europe and therefore with the EU2020 Strategy. 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.

1.6. 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 (esimated 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.

1.7. Management modes envisaged[39]

– ☒ Centralised direct management by the Commission

– ☒ Centralised indirect management with the delegation of implementation tasks to:

– ☐executive agencies

– ☒ bodies set up by the Communities[40]

– ☐ 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:

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

[39] 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

[40] As referred to in Article 185 of the Financial Regulation.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

The Commission willl periodically review the functioning of the Directive and report to the European Parliament and the Council.

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.

2.2. Management and control system

2.2.1. Risk identified

- project implementation delays in building the secure infrastructure

2.2.2. Control methods envisaged

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).

2.2.3. 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.

2.3. 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.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. 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. (41)	from EFTA countries 42	from candidate countries[43]	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/NO	YES/NO	YES/NO	YES/NO

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

42 EFTA: European Free Trade Association.

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

3.2. Estimated impact on expenditure

3.2.1. Summary of estimated impact on expenditure

EUR million (to three decimal places)

Heading of multiannual financial framework:	1	Smart and inclusive Growth

DG: <…….>			2015* [44]	Year **2016**	Year **2017**	Year **2018**	Subsequent years (2019-2021) and beyond			**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[45]			**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					**1.250**

[44] Year N is the year in which implementation of the proposal/initiative starts.

[45] 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 amount is slightly higher than the one mentioned in the Impact Assessment ("about 1 million EUR") as it is based on a more precise estimate of the necessary building blocks for such an infrastructure. The necessary building blocks and their related costs are based on an estimation of the JRC, based on its experience in developing similar systems for other areas like public health, and would comprise the following: a Rapid Alerting and Notification System for NIS (275 000 EUR); an Information Exchange Platform (400 000 EUR); an Early Warning and Response System (275 000 EUR); a Situation Room (300 000 EUR) for a total of 1 250 000 EUR. 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) and beyond			**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**[46]	Year **2016**	Year **2017**	Year **2018**	Subsequent years (2019-2021) and beyond			**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**

[46] Year N is the year in which implementation of the proposal/initiative starts.

3.2.2. 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) and beyond						**TOTAL**	
	OUTPUTS																	
	Type[47]	Average cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Total number	Total cost
SPECIFIC OBJECTIVE NO 2[48] 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

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

48 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).

** See point 3.2.1

3.2.3. Estimated impact on appropriations of an administrative nature

3.2.3.1. 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**[49]	Year **2016**	Year **2017**	Year **2018**	Subsequent years (2019-2021) and beyond			**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 5[50] **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**
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.

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

50 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.

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 resourses allocations.

3.2.3.2. 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 amounts (or at most to one decimal place)

	Year **2015**	Year **2016**	Year **2017**	Year **2018**	Subsequent years (2019-2021) and beyond		
• Establishment plan posts (officials and temporary agents)							
09 01 01 01 (Headquarters and Commission's Representation Offices)	4	4	4	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)[51]							
09 01 02 01 (CA, INT, SNE from the "global envelope")	1	1	1	1	1	1	1
XX 01 02 02 (CA, INT, JED, LA and SNE in the delegations)							
XX 01 04 ***yy*** [52] - at Headquarters[53]							
XX 01 04 ***yy*** [52] - in delegations							
XX 01 05 02 (CA, INT, SNE - Indirect research)							
10 01 05 02 (CA, INT, SNE - Direct research)							
Other budget lines (specify)							
TOTAL	**5**	**5**	**5**	**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

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

52 Under the ceiling for external personnel from operational appropriations (former "BA" lines).

53 Essentially for Structural Funds, European Agricultural Fund for Rural Development (EAFRD) and European Fisheries Fund (EFF).

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 - 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.

3.2.4. 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 on operational expenditure 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 one-off cost 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 framework[54].

Not applicable.

3.2.5. Third-party contributions

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

3.3. Estimated impact on revenue

– ☑ Proposal/initiative has no financial impact on revenue.

[54] See points 19 and 24 of the Interinstitutional Agreement.