EUROPEAN PARLIAMENT 2009 - 2014

Committee on Industry, Research and Energy

2013/0027(COD)

19.12.2013

OPINION

of the Committee on Industry, Research and Energy

for the Committee on the Internal Market and Consumer Protection

on the 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
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Rapporteur(*): del Pilar del Castillo Vera

(*) Associated committee – Rule 50 of the Rules of Procedure

PA_Legam

SHORT JUSTIFICATION

In February 2013 the European Commission, as requested by the European Parliament in its own initiative report on a Digital Agenda for Europe, presented a proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, together with the first EU cyber-security strategy. Taking into account that analysing the available data it can be estimated that ICT-related incidents of a malicious nature could incur direct costs of more than 560 million Euros per year for SMEs alone, and that all types of incidents (including upstream environmental or physical problems such as natural disasters) could incur direct costs of more than 2.3 billion, the Rapporteur warmly welcomes the proposal.

Regarding its structure, the Rapporteur agrees with a number of the proposed measures, such as the extension of the provisions of reporting security incidents currently limited to telecommunications providers under Article 13a of the 2009 Framework Directive to other critical infrastructure sectors. Accordingly, proposals such as requiring that all Member States must have properly functioning computer emergency response teams and designate a competent authority to be part of a secure pan-European electronic data interchange network to permit the secure sharing and exchange of cyber-security related information, are well received and have the potential to greatly contribute to the objective of the proposed Directive, namely to ensure a high common level of network and information security across the Union.

Your Rapporteur is however of the opinion that there is room for improving the proposal, applying the prism of two main principles: Efficiency and Trust.

First Principle - Efficiency

Regarding the obligations on the Member States to designate a competent authority responsible for monitoring the application of the Directive for all the sectors present in Annex II of the proposal, the Rapporteur is of the opinion that each Member State must not only be free to choose the cyber-security governance model it deems most appropriate, but also that it is imperative to avoid duplication of institutional structures that will potentially lead to conflicts of competence and disruption of communications. Accordingly the Rapporteur is of the opinion that existing national structures that are already efficiently in place and respond to Member State needs and constitutional requirements should not be disrupted. She believes however that in order to guarantee the exchange of information at Union level, the notification of early warning threats and the participation in the Cooperation Network in an efficient manner, each Member State must appoint a **Single Point of Contact**.

In the same spirit of maximizing the efficiency of the proposed Directive the Rapporteur is of the opinion that the proposed measures regarding the establishment of a national **Computer Emergency Response Team (CERT)** might not prove to be the most adequate requirement, given that it disregards the different natures and compositions of existing CERTs. Not only do most Member States have more than one CERT, these also deal with different types of incidents. The quantity and quality of activities also differ depending on whether academic or research institutions, governments or the private sector are hosting and operating them. In

addition the current proposal would disrupt existing international and European cooperation networks, to which existing CERTs already belong, which have proven efficient in coordinating international and European responses to incidents. Consequently, your Rapporteur is of the opinion that instead of referring to a single national CERT, the Directive should be targeted to those CERTs that provide their services to the sectors in Annex II, consequently allowing for example that one CERT provides services to all Annex II sectors or that several CERTs provide services to the same sector. The Rapporteur is however of the opinion that Member States must guarantee full operability at all times of their CERTs and guarantee they have sufficient technical, financial and human resources to properly operate and participate in international and union cooperation networks.

The efficiency principle furthermore requires changes to the proposed Directive regarding **the scope**. While the Rapporteur agrees that an extension of the reporting system obligations to the energy, transport, health and financial sectors is needed, the proposal to extend the compulsory measures laid down in Chapter IV to all market operators in the "Internet economy" is disproportionate and unmanageable. Disproportionate because the indiscriminate imposition of new obligations to an open and non-defined category such as every "provider of information society services which enable the provision of other information society services" is not only incomprehensible but also not duly justified with regards to possible damage produced by a security incident, and carries with it the potential to add another layer of bureaucracy to our industrial sector and more particularly to SMEs. Unmanageable, because serious doubts arise to whether competent authorities would be able to cope with all potential notifications in a proactive manner that would encourage a bidirectional dialogue with market operators in order to resolve the security threat.

Regarding **public administrations**, the Directive should balance the need for further development of eGovernment services with the already existing due diligence obligations on public administrations regarding the management and protection of their networks and information systems. Consequently, the Rapporteur is of the opinion that while the exchange of information requirements established in Article 14 should fully apply to public administrations, they should not be subject to the obligations of Article 15.

Second Principle - Trust

The Rapporteur's view is that a great part of the success of the Directive lies in its ability to incentivise participation of market operators, leading to the creation of a trustworthy NIS environment where those that are on the ground are willing to proactively participate. If it does not achieve this, it will fail. In this regard the Rapporteur proposes to guarantee that participation and notification of market operators is not negatively impacted by unnecessary publications of security incidents they have notified, or that they can be held liable for information loss by competent authorities or single points of contact. In addition a bidirectional dialog must be open between operators and competent authorities and participation of the market operators must be encouraged in all fora, including the cooperation network.

The Rapporteur also believes that trust should be the pillar of the participation of the competent authorities and/or the single points of contact, especially regarding the exchange of

information. In order to guarantee this, provisions regarding confidentiality and security requirements of the network should be reflected in the Directive.

AMENDMENTS

The Committee on Industry, Research and Energy calls on the Committee on the Internal Market and Consumer Protection, as the committee responsible, to incorporate the following amendments in its report:

Amendment 1

Proposal for a directive
Recital 1

Text proposed by the Commission	*Amendment*
(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.	(1) Network and information systems and services play a vital role in the society. Their reliability and security are essential to ***the freedom and overall security for the citizens of the EU as well as to*** economic activities and social welfare, and in particular to the functioning of the internal market.

Amendment 2

Proposal for a directive
Recital 2

Text proposed by the Commission	*Amendment*
(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.	(2) The magnitude***,*** frequency ***and impact*** of security incidents is increasing and represents a major threat to the functioning of networks and information systems. ***These systems may also become an easy target for deliberate harmful actions intended to damage or interrupt the operation of the systems.*** Such incidents can ***threaten the health and safety of the population,*** impede the pursuit of economic activities, generate substantial financial losses, undermine user ***and***

	investor confidence and cause major damage to the economy of the Union.

Justification

Cyber attacks on stock listed companies are widespread and include theft of financial assets, intellectual property, or the disruption of operations of their customers or their business partners and could have an impact on shareholder relations as well as on the decision of potential investors.

Amendment 3

Proposal for a directive
Recital 3

Text proposed by the Commission	*Amendment*
(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.	(3) As a communication instrument without ***traditional*** frontiers, digital information systems, and primarily the Internet play an essential role in facilitating the cross-border movement of goods, services***, ideas*** 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 ***and moreover to the functioning of external markets, too***.

Justification

The resilience and stability of network and information systems of the internal market are also vital for the interaction with global and regional markets such as North America or Asia etc.

Amendment 4

Proposal for a directive
Recital 4

Text proposed by the Commission	*Amendment*
(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.	(4) A cooperation mechanism should be established at Union level to allow for information exchange and coordinated ***prevention,*** 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 and private*** operators of information infrastructure ***and companies listed on the stock markets*** to promote a culture of risk management and ensure that the most serious incidents are reported. ***The legal framework should be based upon the need to safeguard the privacy and integrity of citizens. The Critical Infrastructure Warning Information Network (CIWIN) should be expanded to these particular operators.***

Justification

Security breaches of stock listed companies could materially affect the company's products, services, relationships with customers or suppliers, and overall competitive conditions and therefore could have major impacts on the functioning of the internal (and external) market. Therefore stock listed companies should be covered by this Directive as well.

Amendment 5

Proposal for a directive
Recital 4 a (new)

Text proposed by the Commission	*Amendment*
	(4a) This Directive should focus on critical infrastructure essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, financial market infrastructures and health.

Amendment 6

Proposal for a directive
Recital 4 b (new)

Text proposed by the Commission	*Amendment*
	(4b) To secure that governments do not exceed or misuse their powers, it is of vital importance that information and security systems of public authorities are transparent, legitimate, well-defined and adopted in a transparent manner through a democratic process.

Amendment 7

Proposal for a directive
Recital 6

Text proposed by the Commission	*Amendment*
(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.	(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 market operators in turn makes it impossible to set up a global and effective mechanism for cooperation at Union level, ***damaging in addition the effectiveness of international cooperation and consequently the fight against global security challenges, and undermines the Union's leading position internationally in safeguarding and promoting an open, efficient and secure internet***.

Amendment 8

Proposal for a directive
Recital 7

Text proposed by the Commission	*Amendment*
(7) Responding effectively to the challenges 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***.	(7) Responding effectively to the challenges of the security of network and information systems therefore requires a global approach at Union level covering common minimum capacity building and planning requirements, ***developing sufficient cybersecurity skills,*** exchange of information and coordination of actions, and common minimum security requirements. ***Minimal common standards should be applied in accordance with appropriate recommendations by the Cyber Security Co-Ordination Groups (CSGC).***

Amendment 9

Proposal for a directive
Recital 9

Text proposed by the Commission	*Amendment*
(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.	(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***, on the basis of minimum requirements set in this Directive,*** in order to reach capacity response levels allowing for effective and efficient cooperation at national and Union level in case of incidents. ***Each Member State should therefore be obliged to meet***

common standards regarding data format and the exchangeability of data to be shared and evaluated. Member States may ask for the assistance of the European Network and Information Security Agency ('ENISA') in developing their national NIS strategies, based on a common minimum NIS strategy blueprint.

Justification

ENISA is already acknowledged by relevant stakeholders as a highly competent centre of excellence and a trustworthy tool for promoting cybersecurity in the EU. Therefore the EU should avoid duplication of efforts and structures by building upon ENISA's know-how and require ENISA to offer counselling services to those Member States that lack NIS institutions and expertise and make a request for this kind of support.

Amendment 10

Proposal for a directive
Recital 10

Text proposed by the Commission	*Amendment*
(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.	(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 ***single*** focal point for ***both internal coordination and*** cross-border cooperation at Union level should be established or identified in each Member State. These ***single national points of contact should be designated without prejudice for each Member State to designate more than one national competent authority in charge of network information security, according to their constitutional, jurisdictional or administrative requirements, but should nonetheless be assigned with a coordinating mandate at national and Union level. These*** bodies should be given the adequate technical, financial and human resources to ensure that they can carry out in a ***continuous,*** effective and

efficient manner the tasks assigned to them and thus achieve the objectives of this Directive.

Amendment 11

Proposal for a directive
Recital 10 a (new)

Text proposed by the Commission	*Amendment*
	(10a) In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements and to avoid duplication, Member States should be able to designate more than one national competent authority in charge of fulfilling the tasks linked to the security of the networks and information systems of market operators under this Directive. However, in order to ensure smooth cross-border cooperation and communication, it is necessary that each Member State designate only one national single point of contact in charge of cross-border cooperation at Union level. Where its constitutional structure or other arrangements so require, a Member State should be able to designate only one authority to carry out the tasks of the competent authority and the single point of contact.

Amendment 12

Proposal for a directive
Recital 11

Text proposed by the Commission	*Amendment*
(11) All Member States should be adequately equipped, both in terms of technical and organisational capabilities, to prevent, detect, respond to and mitigate	(11) All Member States ***and market operators*** should be adequately equipped, both in terms of technical and organisational capabilities, to prevent,

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.	detect, respond to and mitigate network and information systems' incidents and risks ***at any moment***. ***Security systems of public administrations must be safe and subject to democratic control and scrutiny. Commonly required equipment and capabilities ought to comply with commonly agreed technical standards as well as standards procedures of operation (SPO).*** Well-functioning Computer Emergency Response Teams ***(CERTs)*** 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. ***These CERTs should be enabled to interact on the basis of common technical standards and SPO. In view of the different characteristics of existing CERTs, which responds to different subject needs and actors, Member States should guarantee that each of the sectors covered by Annex II is provided services by at least one CERT. Regarding cross border CERT cooperation, Member States should assure that CERTs have sufficient means to participate in the existing international and European cooperation networks already in place.***

Justification

Interoperability has to be ensured.

Amendment 13

Proposal for a directive
Recital 12

Text proposed by the Commission	*Amendment*
(12) Building upon the significant progress within the European Forum of Member States (***'EFMS'***) in fostering discussions and exchanges on good policy practices	(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.	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***, where the participation of market operators is assured,*** should enable structured and coordinated information exchange, detection and response at Union level.

Amendment 14

Proposal for a directive
Recital 13

Text proposed by the Commission	*Amendment*
(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.	(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 ***and Member States*** 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.

Amendment 15

Proposal for a directive
Recital 14

Text proposed by the Commission	*Amendment*
(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.	(14) A secure information-sharing infrastructure should be put in place***, under the supervision of ENISA,*** 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. ***In order for the cooperation network to be able to efficiently fulfil its mission, the Commission should establish a budget line for the network.***

Amendment 16

Proposal for a directive
Recital 14 a (new)

Text proposed by the Commission	*Amendment*
	(14a) Where appropriate, market operators may also be invited to participate in the activities of the cooperation network.

Amendment 17

Proposal for a directive
Recital 15

Text proposed by the Commission	*Amendment*
(15) As most network and information systems are privately operated, cooperation	(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.

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 ***mutually*** share information and best practices ***including the reciprocal*** in exchange of ***relevant information and*** operational support ***and strategically analysed information,*** in case of incidents. ***To effectively encourage the sharing of information and of best practices, it is essential to ensure that market operators, who participate in such exchanges, are not disadvantaged as a result of their cooperation. Adequate safeguards are needed to ensure that such cooperation will not expose these operators to higher compliance risk or new liabilities under, inter alia, competition, intellectual property, data protection or cybercrime law, nor expose them to increase operational or security risks.***

Amendment 18

Proposal for a directive
Recital 16

Text proposed by the Commission	*Amendment*
(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.	(16) To ensure transparency and properly inform EU citizens and market operators, ***the single points of contact*** should set up a common ***Union-wide*** website to publish non confidential information on the incidents, ***risks and ways of risk mitigation, and to eventually advise on appropriate maintenance measures***.

Amendment 19

Proposal for a directive
Recital 17

Text proposed by the Commission	*Amendment*
(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.	(17) ***The information classification policy referred to in Recital 14 should follow the ENISA recommended Information Sharing Traffic Light Protocol. Any information exchanged shall be classified and handled according to its level of sensitivity as determined by the source of the information.*** 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.

Amendment 20

Proposal for a directive
Recital 18

Text proposed by the Commission	*Amendment*
(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.	(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***, best practices and operation patterns*** to ***prevent, detect, report, and*** counter risks and incidents. That plan should be duly taken into account in the operation of early warnings within the cooperation network.

Amendment 21

Proposal for a directive
Recital 19

Text proposed by the Commission	*Amendment*
(19) Notification of an early warning	(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.

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 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.

Amendment 22

Proposal for a directive
Recital 20

Text proposed by the Commission	*Amendment*
(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.	(20) Upon receipt of an early warning and its assessment, the ***single points of contact*** should agree on a coordinated response under the Union NIS cooperation plan. ***The single points of contact, ENISA*** as well as the Commission should be informed about the measures adopted at national level as a result of the coordinated response.

Amendment 23

Proposal for a directive
Recital 22

Text proposed by the Commission	*Amendment*
(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	(22) Responsibilities in ensuring NIS lie to a great extent on public administrations and market operators. A culture of risk management***, close cooperation and trust***, involving risk assessment and the implementation of security measures appropriate to the risks faced should be

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.

promoted and developed through appropriate regulatory requirements and voluntary industry practices. Establishing a ***trustworthy*** level playing field is also essential to the effective functioning of the cooperation network to ensure effective cooperation from all Member States.

Amendment 24

Proposal for a directive
Recital 24

Text proposed by the Commission	*Amendment*
(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[27], 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***	(24) Those obligations should be extended beyond the electronic communications sector ***to operators of 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, financial market infrastructures and health. Disruption of those network and information systems would affect the internal market. While the obligations set out in this directive do not extend*** 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[27], 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 ***in general or*** application stores***,*** these ***may, on a voluntary basis, inform the competent authority or single point of contact of*** those ***network security incidents they deem appropriate, and the competent authority or the single point of contact***

network and information ***systems would affect the internal market***.	***should, if reasonably possible, present the market operators that informed of the incident with strategically analysed*** information ***that will help overcome the security threat***.
[27] OJ L 204, 21.7.1998, p. 37.	[27] OJ L 204, 21.7.1998, p. 37.

Amendment 25

Proposal for a directive
Recital 25

Text proposed by the Commission	*Amendment*
(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.	(25) Technical and organisational measures imposed to market operators should not require that a particular commercial information and communications technology product be designed, developed or manufactured in a particular manner. ***On the other hand, the use of international standards pertaining to cybersecurity should be required.***

Amendment 26

Proposal for a directive
Recital 28

Text proposed by the Commission	*Amendment*
(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	(28) Competent authorities ***and single points of contact*** should pay due attention to preserving informal and trusted channels of information-sharing between market operators and between the public and the private sectors. ***Previously unknown vulnerabilities or incidents reported to competent authorities should be notified to the manufacturers and service providers of affected ICT products and services.*** Publicity of incidents reported to

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.

the competent authorities ***and single points of contact*** should duly balance the interest of the public in being informed about threats with possible reputational and commercial damages for the market operators reporting incidents. In ***order to safeguard trust and efficiency, publicity of incidents shall only take place after consultation with those who reported the incident and only when strictly necessary for achieving the objectives of this Directive. In*** the implementation of the notification obligations, competent authorities ***and single points of contact*** should pay particular attention to the need to maintain information about product vulnerabilities strictly confidential prior to the ***deployment*** of appropriate security fixes ***though not delay any notification more than compulsorily required***. ***As a general rule, single points of contact should not disclose personal data of individuals involved in incidents. Single points of contact should only disclose personal data where the disclosure of such data is necessary and proportionate in view of the objective pursued.***

Justification

In case authorities are aware of vulnerabilities of certain ICT products or services, they should notify the manufacturers and service providers in order to allow them to adapt their products and services in a timely manner.

Amendment 27

Proposal for a directive
Recital 29

Text proposed by the Commission	*Amendment*
(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	(29) Competent authorities ***and single points of contact*** should have the necessary means to perform their duties, including powers to obtain sufficient information from market operators in order

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.	to assess the level of security of network and information systems***, measure the number, scale and scope of incidents,*** as well as reliable and comprehensive data about actual incidents that have had an impact on the operation of network and information systems.

Amendment 28

Proposal for a directive
Recital 30

Text proposed by the Commission	*Amendment*
(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.	(30) Criminal ***or cyberwar*** 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***, single points of contact*** and law enforcement authorities ***as well as cooperation with the EC3 (Europol Cybercrime Centre) and ENISA*** 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.

Amendment 29

Proposal for a directive
Recital 31

Text proposed by the Commission	*Amendment*
(31) Personal data are in many cases	(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[28] . 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.

compromised as a result of incidents. ***Member States and market operators should protect personal data stored, processed or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, access or disclosure, dissemination, or access; and ensure the implementation of a security policy with respect to the processing of personal data.*** In this context, competent authorities***, single points of contact*** and data protection authorities should cooperate and exchange information on all relevant matters to tackle the personal data breaches resulting from incidents. The obligation to notify security incidents ***should be carried out*** in a way that minimises the administrative burden in case the security incident is also a personal data breach ***that is required to be notified in accordance with applicable law.*** ENISA ***should*** assist by developing information exchange mechanisms and ***a*** single notification template ***that*** would facilitate the reporting of incidents compromising personal data thereby easing the administrative burden on businesses and public administrations.

[28] SEC(2012) 72 final

Justification

Aligned to the draft Data Protection Directive.

Amendment 30

Proposal for a directive
Recital 32

Text proposed by the Commission	*Amendment*
(32) Standardisation of security requirements is a market-driven process.	(32) Standardisation of security requirements is a market-driven process ***of***

To ensure a convergent application of security standards, Member States should encourage 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[29] .

[29] OJ L 316, 14.11.2012, p. 12.

a voluntary nature that should allow market operators to use alternative means to achieve at least similar outcomes. To ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified ***interoperable*** standards to ensure a high level of security at Union level. To this end, ***the application of open international standards on network information security or the design of such tools need to be considered. Another necessary step forward*** might be 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[29]. ***In particular, ETSI, CEN and CENELEC should be mandated to suggest effective and efficient EU open security standards, where technological preferences are avoided as much as possible, and which should be made easily manageable by small and medium-size market operators. International standards pertaining to cybersecurity should be carefully vetted in order to ensure that they have not been compromised and that they provide adequate levels of security, thus safeguarding that the mandated compliance with cybersecurity standards enhances the overall level of cybersecurity of the Union and not the contrary.***

[29] OJ L 316, 14.11.2012, p. 12.

Amendment 31

Proposal for a directive
Recital 33

Text proposed by the Commission	*Amendment*
(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**.**	(33) The Commission should periodically review this Directive, in ***consultation with all interested stakeholders, in*** particular with a view to determining the need for modification in the light of changing ***societal, political,*** technological or market conditions

Amendment 32

Proposal for a directive
Recital 34

Text proposed by the Commission	*Amendment*
(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.	***deleted***

Amendment 33

Proposal for a directive
Recital 35

Text proposed by the Commission	*Amendment*
(35) It is of particular importance that the	(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.	Commission carry out appropriate consultations during its preparatory work, including ***all stakeholders and in particular*** at expert level. The Commission should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

Amendment 34

Proposal for a directive
Recital 36

Text proposed by the Commission	*Amendment*
(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[30] .	(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 ***single points of contact*** and the Commission within the cooperation network, ***without prejudice to existing cooperation mechanisms at national level, the common set of interconnection and security standards for*** the secure information-sharing infrastructure, the Union NIS cooperation plan ***and*** the formats and procedures applicable to ***notifying significant*** incidents. 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[30].
[30] OJ L 55, 28.2.2011, p.13.	[30] OJ L 55, 28.2.2011, p.13.

Amendment 35

Proposal for a directive
Recital 37

Text proposed by the Commission	*Amendment*
(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.	(37) In the application of this Directive, the Commission should liaise as appropriate with relevant sectorial committees and relevant bodies set up at EU level in particular in the field of ***e-Government,*** energy, transport and health.

Amendment 36

Proposal for a directive
Recital 38

Text proposed by the Commission	*Amendment*
(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.	(38) Information that is considered confidential by a competent authority ***or a single point of contact***, in accordance with Union and national rules on business confidentiality, should be exchanged with the Commission, ***its relevant agencies, single points of contact and/or other national 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***, necessary*** and proportionate to the purpose of such exchange***, while respecting pre-defined criteria for confidentiality and security and classification protocols, governing the information sharing procedure***.

Amendment 37

Proposal for a directive
Recital 39

Text proposed by the Commission	*Amendment*
(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 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[31] 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.	(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 ***or single points of contact*** may require the processing of personal data. Such a processing of personal 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[31] 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.
[31] OJ L 145, 31.5.2001, p. 43.	[31] OJ L 145, 31.5.2001, p. 43.

Amendment 38

Proposal for a directive
Recital 41 a (new)

Text proposed by the Commission	*Amendment*
	(41a) 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.

Amendment 39

Proposal for a directive
Article 1 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(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;	(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 ***with the participation of relevant stakeholders***;

Amendment 40

Proposal for a directive
Article 1 – paragraph 6

Text proposed by the Commission	*Amendment*
6. The sharing of information within the cooperation network under Chapter III and the notifications of NIS incidents under	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 14 may require the ***communication to trusted third parties and 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. ***Member States shall adopt legislative measures in accordance with Article 13 of Directive 95/46/EC to ensure that public administrations, market operators and competent authorities are not held liable for processing personal data, necessary for the sharing of information within the cooperation network and incident notification.***

Amendment 41

Proposal for a directive
Article 2 – paragraph 1

Text proposed by the Commission	*Amendment*
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.	Member States shall not be prevented from adopting or maintaining provisions ensuring a higher level of security ***that conform to the Charter of Fundamental Rights of the European Union***, without prejudice to their obligations under Union law.

Justification

The leeway that Member States enjoy on matters of security must be conditional on respect for the principles set out in the Charter of Fundamental Rights of the European Union, including for example the right to respect for private life and communications, to protection of personal data, to freedom to conduct a business and to effective remedy before a court.

Amendment 42

Proposal for a directive
Article 3 – paragraph 1 – point 1 – point b

Text proposed by the Commission	*Amendment*
(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	(b) any device or group of inter-connected or related devices, one or more of which, pursuant to a program, perform automatic processing of ***digital*** data, as well as

Amendment 43

Proposal for a directive
Article 3 – paragraph 1 – point 1 – point c

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

Amendment 44

Proposal for a directive
Article 3 – paragraph 1 – point 2

Text proposed by the Commission	*Amendment*
(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;	(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; ***"security" as defined here includes appropriate technical devices, solutions and operating procedures ensuring the security requirements set forth in this Directive.***

Amendment 45

Proposal for a directive
Article 3 – paragraph 1 – point 4

Text proposed by the Commission	*Amendment*
(4) 'incident' means any circumstance or event having an actual adverse effect on security;	(4) 'incident' means any ***reasonably identifiable*** circumstance or event having an actual adverse effect on security;

Justification

The original wording was too broad and would have complicated application of the definition.

Amendment 46

Proposal for a directive
Article 3 – paragraph 1 – point 5

Text proposed by the Commission	*Amendment*
(5) 'information society service' mean service within the meaning of point (2) of Article 1 of Directive 98/34/EC;	***deleted***

Amendment 47

Proposal for a directive
Article 3 – paragraph 1 – point 8 – point a

Text proposed by the Commission	*Amendment*
(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;	***deleted***

Amendment 48

Proposal for a directive
Article 3 – paragraph 1 – point 7

Text proposed by the Commission	*Amendment*
(7) 'incident handling' means all procedures supporting the analysis, containment and response to an incident;	(7) 'incident handling' means all procedures supporting the ***detection, prevention,*** analysis, containment and response to an incident;

Amendment 49

Proposal for a directive
Article 3 – paragraph 1 – point 8

Text proposed by the Commission	*Amendment*
(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.	(b) ***public or private*** operator of infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, ***financial markets*** and health***, and the disruption or destruction of which would have a significant negative impact in a Member State as a result of the failure to maintain those functions***, a list of which is set out in Annex II.

Amendment 50

Proposal for a directive
Article 3 – paragraph 1 – point 8 a (new)

Text proposed by the Commission	*Amendment*
	(8a) "incident having a significant

impact" means an incident affecting the security and continuity of an information network or system that leads to the major disruption of vital economic or societal functions;

Amendment 51

Proposal for a directive
Article 3 – paragraph 1 – point 8 b (new)

Text proposed by the Commission	*Amendment*
	(8b) 'service' means the service provided by a market operator, to the exclusion of any other services of the same entity.

Amendment 52

Proposal for a directive
Article 3 – paragraph 1 – point 11 a (new)

Text proposed by the Commission	*Amendment*
	(11a) 'regulated market' means regulated market as defined in point 14 of Article 4 of Directive 2004/39/EC of the European Parliament and of the Council[28a];
	[28a] Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments (OJ L 45, 16.2.2005, p. 18).

Amendment 53

Proposal for a directive
Article 3 – paragraph 1 – point 11 b (new)

Text proposed by the Commission	*Amendment*
	(11b) 'multilateral trading facility (MTF)' means multilateral trading facility as

defined in point 15 of Article 4 of Directive 2004/39/EC;

Amendment 54

Proposal for a directive
Article 3 – paragraph 1 – point 11 c (new)

Text proposed by the Commission	*Amendment*
	(11c) 'organised trading facility' means a multilateral system or facility, which is not a regulated market, a multilateral trading facility or a central counterparty, operated by an investment firm or a market operator, in which multiple third-party buying and selling interests in bonds, structured finance products, emission allowances or derivatives are able to interact in the system in a way that results in a contract in accordance with the provisions of Title II of Directive 2004/39/EC;

Amendment 55

Proposal for a directive
Article 4 – paragraph 1

Text proposed by the Commission	*Amendment*
Member States shall ensure a high level of security of the network and information systems in their territories in accordance with this Directive.	Member States shall ensure a ***sustained continuous*** high level of security of the network and information systems in their territories in accordance with ***the Charter of Fundamental Rights of the European Union and*** this Directive.

Justification

The leeway that Member States enjoy on matters of security must be conditional on respect for the principles set out in the Charter of Fundamental Rights of the European Union, including for example the right to respect for private life and communications, to protection of personal data, to freedom to conduct a business and to effective remedy before a court.

Amendment 56

Proposal for a directive
Article 5 – paragraph 1 – point e a (new)

Text proposed by the Commission	*Amendment*
	(ea) Member States may ask for the assistance of the European Network and Information Security Agency ('ENISA') in developing their national NIS strategies and national NIS cooperation plans, based on a common minimum NIS strategy and cooperation blueprint.

Amendment 57

Proposal for a directive
Article 5 – paragraph 2 – point a

Text proposed by the Commission	*Amendment*
(a) A risk ***assessment plan to identify risks and assess*** the impacts of potential incidents;	(a) A risk ***management framework including the identification, prioritisation, evaluation and treatment of risks, the assessment of*** the impacts of potential incidents***, prevention and control options, and criteria for the choice of possible countermeasures***;

Amendment 58

Proposal for a directive
Article 5 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) The definition of the roles and responsibilities of the various actors involved in the implementation of the ***plan***;	(b) The definition of the roles and responsibilities of the various ***authorities and other*** actors involved in the implementation of the ***framework***;

Amendment 59

Proposal for a directive
Article 6 – title

Text proposed by the Commission	*Amendment*
National competent ***authority*** on the security of network and information systems	National competent ***authorities and single points of contact*** on the security of network and information systems

Amendment 60

Proposal for a directive
Article 6 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Each Member State shall designate ***a*** national competent ***authority*** on the security of network and information systems (***the*** 'competent authority').	1. Each Member State shall designate ***one or more*** national competent ***authorities*** on the security of network and information systems (***hereinafter referred to as the*** 'competent authority').

Amendment 61

Proposal for a directive
Article 6 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2a. Where a Member State designates more than one competent authority, it shall designate a national authority, for instance a competent authority, as national single point of contact on the security of network and information systems (hereinafter referred to as "single point of contact"). Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact.

Amendment 62

Proposal for a directive
Article 6 – paragraph 2 b (new)

Text proposed by the Commission	*Amendment*
	2b. The competent authorities and the single point of contact of the same Member State shall cooperate closely with regard to the obligations laid down in this Directive.

Amendment 63

Proposal for a directive
Article 6 – paragraph 2 c (new)

Text proposed by the Commission	*Amendment*
	2c. The single point of contact shall ensure cross-border cooperation with other single points of contact.

Amendment 64

Proposal for a directive
Article 6 – paragraph 3

Text proposed by the Commission	*Amendment*
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.	3. Member States shall ensure that the competent authorities ***and the single points of contact*** 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 ***single points of contact*** via the network referred to in Article 8.

Amendment 65

Proposal for a directive
Article 6 – paragraph 4

Text proposed by the Commission	*Amendment*
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.	4. Member States shall ensure that the competent authorities ***and single points of contact*** receive the notifications of incidents from market operators as specified under Article 14(2) and are granted the implementation and enforcement powers referred to under Article 15.

Amendment 66

Proposal for a directive
Article 6 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The competent authorities shall consult and cooperate, whenever appropriate, with the relevant law enforcement ***national authorities and data protection*** authorities.	5. The competent authorities shall consult ***with the data protection authorities as a matter of course*** and cooperate, whenever appropriate, with the relevant ***national*** law enforcement authorities.

Justification

The balance between ensuring security and safeguarding freedoms would be upset were just a single authority to exercise monitoring power at national level without the cooperation of another, compensating body.

Amendment 67

Proposal for a directive
Article 6 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The competent authorities shall consult and cooperate, whenever appropriate, with the relevant law enforcement national authorities and data protection authorities.	5. The competent authorities ***and single points of contact*** shall consult and cooperate, whenever appropriate, with the relevant law enforcement national

authorities and data protection authorities.

Amendment 68

Proposal for a directive
Article 6 – paragraph 6

Text proposed by the Commission	*Amendment*
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***.	6. Each Member State shall notify to the Commission without delay the designation of the competent ***authorities and the single point of contact***, its tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent ***authorities***.

Amendment 69

Proposal for a directive
Article 7 – paragraph 1

Text proposed by the Commission	*Amendment*
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.	1. Each Member State shall set up ***at least one*** Computer Emergency Response Team (hereinafter: ***"CERT"***) ***for each of the sectors established in Annex II,*** 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.

Amendment 70

Proposal for a directive
Article 7 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The ***CERT*** shall act under the supervision of the competent authority, which shall regularly review the adequacy	5. The ***CERTs*** shall act under the supervision of the competent authority ***or the single point of contact***, which shall

of ***its*** resources, ***its*** mandate and the effectiveness of ***its*** incident-handling process.	regularly review the adequacy of ***their*** resources, ***mandates*** and the effectiveness of ***their*** incident-handling process.

Amendment 71

Proposal for a directive
Article 7 – paragraph 5 a (new)

Text proposed by the Commission	*Amendment*
	5a. Member States shall ensure that CERTs have adequate human and financial resources to actively participate in international, and in particular Union, cooperation networks

Amendment 72

Proposal for a directive
Article 7 – paragraph 5 – point 1 (new)

Text proposed by the Commission	*Amendment*
	(1) The CERTs shall be enabled and encouraged to initiate and to participate in joint exercises with other CERTs, with all Member States-CERTs, and with appropriate institutions of non-Member States as well as with CERTs of multi- and international institutions such as NATO and the UN.

Amendment 73

Proposal for a directive
Article 7 – paragraph 5 a (new)

Text proposed by the Commission	*Amendment*
	5a. Member States may ask for the assistance of the European Network and Information Security Agency ('ENISA')

	or of other Member States in developing their national CERTs.

Amendment 74

Proposal for a directive
Article 8

Text proposed by the Commission	*Amendment*
1. The ***competent authorities*** and the Commission shall form a network (‘cooperation network’) to cooperate against risks and incidents affecting network and information systems.	1. The ***single points of contact, the European Network and Information Security Agency (ENISA)*** and the Commission shall form a network ('cooperation network') ***where they shall*** 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.	2. The cooperation network shall bring into permanent communication the Commission and ***the single points of contact. The*** European Network and Information Security Agency ('ENISA') shall assist the cooperation network by providing its expertise and advice. ***Where relevant, the cooperation network shall cooperate with the data protection authorities.***
3. Within the cooperation network the ***competent authorities*** shall:	3. Within the cooperation network the ***single points of contact*** shall:
(a) circulate early warnings on risks and incidents in accordance with Article 10;	(a) circulate early warnings on risks and incidents in accordance with Article 10;
(b) ensure a coordinated response in accordance with Article 11;	(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;	(c) publish on a regular basis non-confidential information on on-going early warnings and coordinated response on a common website;
	(ca) jointly discuss, agree on a common interpretation, consistent application and coordinate their measures regarding security requirements and incident notification referred to in Article 14 and regarding implementation and enforcement referred to in Article 15;

(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.	(d) jointly discuss and assess 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;	(e) jointly discuss and assess, at the request of ***ENISA,*** a Member State or the Commission, the effectiveness of the CERTs, in particular when NIS exercises are performed at Union level ***and implement measures to resolve identified weaknesses without undue delay***;
(f) cooperate and exchange information on all relevant matters ***with the European Cybercrime Center within Europol, and*** with other relevant European bodies in particular in the fields of *data protection*, energy, transport, banking, ***stock exchanges*** and health;	(f) cooperate and exchange information on all relevant matters ***on network and information security*** with other relevant European bodies in particular in the fields of energy, transport, banking, ***financial markets*** and health;
	(fa) jointly discuss and agree on the common interpretation, consistent application and harmonious implementation within the Union of the provisions of Chapter IV;
(g) exchange information and best practices between themselves and the Commission, and assist each other in building capacity on NIS;	(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;	(h) organise regular peer reviews on capabilities and preparedness;
(i) organise NIS exercises at Union level and participate, as appropriate, in international NIS exercises.	(i) organise NIS exercises at Union level and participate, as appropriate, in international NIS exercises.
	(ia) actively promote involvement of, and consult and exchange information with, market operators.
	The Commission shall regularly inform the cooperation network of security research and other relevant programmes of Horizon2020.
	3a. Where appropriate, relevant public administration and market operators shall be invited to participate in the activities of

	the cooperation network referred to in points (c), (g), (h) and (i) of paragraph 3.
	3b. Where information, early warnings or best practices originating from market operators or public administrations are shared within, or disclosed by the cooperation network, such sharing or disclosure shall be in accordance with the information classification as determined by the original source in accordance with Article 9(1).
	3c. The Commission shall yearly publish a report, based on the activities of the network and on the summary report submitted in accordance with Article 14(4) of this Directive, for the preceding 12 months. Publicity of any individual incidents reported to the competent authorities and single points of contact should duly balance the interest of the public in being informed about threats with possible reputational and commercial damages for the market operators that reported them and can only take place after prior consultation.
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).	4. The Commission shall establish, by means of implementing acts, the necessary modalities to facilitate the cooperation between ***the single points of contact, ENISA*** 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).

Amendment 75

Proposal for a directive
Article 9 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The exchange of sensitive and confidential information within the	1.The exchange of sensitive and confidential information within the

cooperation network shall take place through a secure infrastructure.	cooperation network shall take place through a secure infrastructure ***operated under the supervision of ENISA***. ***Member States shall ensure that shared sensitive or secret information from other States or the Commission will not be shared with third States or improper purposes, for example covert operations or financial decision making.***

Amendment 76

Proposal for a directive
Article 9 – paragraph 2 – introductory part

Text proposed by the Commission	*Amendment*
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:	2. The Commission shall be empowered to adopt ***implementing*** acts in accordance with Article ***19*** concerning the definition of the criteria to be fulfilled for a ***single point of contact*** to be authorized to participate to the secure information-sharing system, regarding:

Amendment 77

Proposal for a directive
Article 9 – paragraph 3

Text proposed by the Commission	*Amendment*
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).	3. The Commission shall adopt, by means of implementing acts, ***a common set of interconnections and security standards that single points of contact must meet in order to exchange information***. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).

Amendment 78

Proposal for a directive
Article 10

Text proposed by the Commission	*Amendment*
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:	1. The ***single points of contact*** 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***;***	(b) ***the single point of contact assesses that the risk or incident grows rapidly or may grow rapidly in scale and potentially exceeds*** national response capacity;
(c) ***they affect or may affect*** more than one Member State.	(c) ***the single points of contact or the Commission assess that the risk or incident affects*** 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.	2. In the early warnings, the ***single points of contact*** and the Commission shall communicate ***without undue delay*** any relevant information in their possession that may be useful for assessing the risk or incident. ***Information deemed classified or confidential by the concerned market operator and the identity of the market operator shall be provided to the degree necessary to assess 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.	3. At the request of a Member State, or on its own initiative, the Commission may request a Member State to provide any relevant ***non-classified*** 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.	4. Where the risk or incident subject to an early warning is of a suspected ***serious*** criminal nature, the ***single points of contact*** or the Commission shall, ***where appropriate, liaise with national cybercrime authorities to enable them to cooperate and exchange information with*** the European Cybercrime Centre within

	Europol ***without undue delay***.
	4 a. Members of the cooperation network shall not make public any information received on risks and incidents according to paragraph 1 without having received the prior approval of the notifying single point of contact.
	4b. Where the risk or incident subject to an early warning is of a suspected severe cross-border technical nature, the single points of contact or the Commission shall inform ENISA;
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.	5. The Commission shall be empowered to adopt ***implementing*** acts in accordance with Article ***19***, concerning the further specification of the risks and incidents triggering early warning referred to in paragraph 1***, as well as the procedures for sharing sensitive information for market operators***.

Amendment 79

Proposal for a directive
Article 11 – paragraph 1

Text proposed by the Commission	*Amendment*
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.	1. Following an early warning referred to in Article 10 the ***single points of contact*** shall, after assessing the relevant information, agree ***without undue delay*** on a coordinated response in accordance with the Union NIS cooperation plan referred to in Article 12.

Amendment 80

Proposal for a directive
Article 12 – paragraph 2 – point a – indent 1

Text proposed by the Commission	*Amendment*
– a definition of the format and procedures	– 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***,	for the collection and sharing of compatible and comparable information on risks and incidents by the ***single points of contact***,

Amendment 81

Proposal for a directive
Article 12 – paragraph 3

Text proposed by the Commission	*Amendment*
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.	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. ***Results of each revision shall be reported to the European Parliament.***

Amendment 82

Proposal for a directive
Article 12 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. The Commission shall provide a budget for the development of the Union NIS cooperation plan.

Amendment 83

Proposal for a directive
Article 13 – paragraph 1

Text proposed by the Commission	*Amendment*
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	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.	participation in some activities of the cooperation network. ***These agreements shall set out the monitoring procedure that must be followed to guarantee the protection of*** personal data circulating on the cooperation network. ***The European Parliament shall be informed on the negotiation of the agreements, the transparency of which shall be guaranteed. Any transfer of personal data to recipients located in countries outside the Union shall be conducted in accordance with Articles 25 and 26 of Directive 95/46/EC and Article 9 of Regulation (EC) No 45/2001.***

Justification

International agreements concluded with other countries or security bodies must contain a monitoring method that guarantees respect for civil rights. Effective democratic oversight of the agreements must also be exercised by the European Parliament, which must be duly informed of the content of the negotiations on the agreements.

Amendment 84

Proposal for a directive
Article 14

Text proposed by the Commission	*Amendment*

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.

1. Member States shall ensure that market operators take appropriate technical and organisational measures to ***detect and effectively*** manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to ***technological development***, these ***appropriate*** measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent ***incidents affecting the security of the network and information systems*** and minimise ***their*** impact 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.

2. Member States shall ***implement mechanisms to*** ensure ***that*** market operators***,*** notify ***without undue delay*** to the competent authority ***or to the single point of contact*** incidents having an impact on the ***security or continuity*** of the core services they provide. ***Notification shall not expose the notifying party to increased liability. To determine the significance of the impact of an incident, the following parameters shall inter alia be taken into account:***

(a) the number of users whose core service is affected;

(b) the duration of the incident;

(c) geographic spread with regard to the area affected by the incident.

These criteria shall be further specified according to Article 8 paragraph 3 point (ca) (new).

2a. Entities not covered by Annex II may report incidents as specified in Article 14(2) on a voluntary basis.

2b. The recipient of an incident report shall, as soon as possible, report back to the entity which reported an incident the undertaken actions, decisions or

recommendations, as well as of any third party informed, and the security and confidentiality protocols governing the information sharing.

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

3. The requirements under paragraphs 1 and 2 apply to all market operators providing services within the European Union. ***Market operators not providing services in the European Union may report incidents on a voluntary basis.***

3a. Member States shall ensure that Market operators notify the incidents referred to in paragraphs 1 and 2 to the competent authority or the single point of contact in the Member State where the core service is affected. Where core services in more than one Member State are affected, the single point of contact which has received the notification shall, based on the information provided by the market operator, alert the other single points of contact concerned. The market operator shall be informed, as soon as possible, which other single points of contact have been informed of the incident, as well as of any undertaken steps, results and any other information with relevance to the incident.

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.

4. ***After consultation with*** the competent authority ***and market operator concerned, the single point of contact shall*** inform the public ***about individual incidents, where it determines that public awareness is necessary to prevent an incident or deal with an ongoing incident, to enable members of the public to mitigate risks to themselves arising from the incident or where the market operator, subject to an incident, has refused to address a serious structural vulnerability related to that incident without undue delay. The single point of contact shall properly justify that decision. The competent authority or the single point of contact shall, if reasonably possible, present market operators that informed of the incident with strategic***

	analysed information that will help overcome the security threat. Twice a year, the ***single point of contact*** shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph. ***Publicity of any individual incidents reported to the competent authorities and single points of contact should duly balance the interest of the public in being informed about threats with possible reputational and commercial damages for market operators that reported them and can only take place after prior consultation.***
	In case of incidents notified to the cooperation network referred to in Article 8, other national competent authorities shall not make public any information received on risks or incidents without approval of the notifying competent authority
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.	6. The competent authorities ***or the single points of contact shall*** adopt guidelines concerning the circumstances in which 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).	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	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[35].

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

2003 concerning the definition of micro, small and medium-sized enterprises[35].

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

Amendment 85

Proposal for a directive
Article 14 – paragraph 4 – subparagraph 1 (new)

Text proposed by the Commission	*Amendment*
	Besides reporting to the competent authority market operators shall be encouraged to announce incidents involving their corporation in their financial reports on a voluntary basis.

Justification

Cyber incidents could imply major financial losses and substantial costs. Shareholder and investors ought to be informed about the consequences of these incidents. By encouraging companies to publish cyber incidents on a voluntary basis the cross-sectoral discussion on the likeliness of future incidents, the dimension of those risks, as well as the appropriateness of preventive actions taken to reduce cyber security breaches might be stimulated.

Amendment 86

Proposal for a directive
Article 15

Text proposed by the Commission	*Amendment*
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.	1. Member States shall ensure that the competent authorities ***and the single points of contact have*** the powers necessary to ***ensure*** compliance with ***the*** 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***	2. Member States shall ensure that the competent authorities ***and the single points of contact*** have the power to require

administrations to:	market operators to:
(a) provide information needed to assess the security of their networks and information systems, including documented security policies;	(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.	(b) ***provide evidence of effective implementation of security policies, such as results of*** a security audit carried out by ***internal auditors,*** a qualified independent body or national authority***,*** and make the ***evidence*** available to the competent authority ***or to the single point of contact. Where necessary, the competent authority or the single point of contact may request additional evidence or exceptionally, and providing due justification, carry out an additional audit.*** ***When sending that request, the competent authorities and the single points of contact shall state the purpose of the request and sufficiently specify what information is required.***
3. Member States shall ensure that competent authorities have the power to issue binding instructions to market operators ***and public administrations***.	3. Member States shall ensure that ***the*** competent authorities ***and the single points of contact*** have the power to issue binding instructions to ***all*** market operators ***laid down in Annex II***.
4. The competent authorities shall ***notify*** incidents of a suspected serious criminal nature ***to*** law enforcement authorities.	4. The competent authorities ***and the single point of contact*** shall ***inform the concerned market operators about the possibility to bring*** criminal ***charges to the*** law enforcement authorities ***in case of incidents of a suspected serious criminal nature***.
5. The competent authorities shall work in close cooperation with personal data protection authorities when addressing incidents resulting in personal data breaches.	5. ***Without prejudice to applicable data protection law, t***he competent authorities ***and the single points of contact*** shall work in close cooperation with personal data protection authorities when addressing incidents resulting in personal data breaches. ***The single points of contact and the data protection authorities shall develop, in cooperation with ENISA, information exchange mechanisms and a single template to be used both for***

	notifications under Article 14(2) of this Directive and Regulation 95/46 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.
	The Commission may adopt, by means of implementing acts and taking the utmost account of any information exchange mechanisms and single template developed by the single points of contact and the data protection authorities, in cooperation with ENISA, procedures for the information exchange mechanisms and the format of the single template.
6. Member States shall ensure that any obligations imposed on ***public administrations and*** market operators under this Chapter may be subject to judicial review.	6. Member States shall ensure that any obligations imposed on market operators under this Chapter may be subject to judicial review.

Amendment 87

Proposal for a directive
Article 16

Text proposed by the Commission	*Amendment*
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.	1. To ensure convergent implementation of Article 14(1), Member States***, without prescribing the use of any particular technology,*** shall encourage the use ***of open EU and international interoperable*** standards and/or specifications relevant to networks and information security***, complying with EU legislation***.
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.	2. The Commission shall ***give a mandate to a relevant European standardisation body to***, ***in consultation with relevant stakeholders,*** draw up a list of the standards ***and/or specifications*** referred to in paragraph 1. The list shall be published in the Official Journal of the European Union.

Amendment 88

Proposal for a directive
Article 17 – paragraph 1

Text proposed by the Commission	*Amendment*
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.	1. Member States shall lay down rules on sanctions applicable to ***negligent and intentional*** 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.

Justification

It should be clear that penalties can only be applied to infringements where market operators have failed to take all measures that could have been reasonable expected of them. Market operators could otherwise be discouraged from reporting incidents.

Amendment 89

Proposal for a directive
Article 17 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	1a. Member States shall ensure that the penalties referred to in paragraph 1 of this article only apply where the market operator has failed to fulfil its obligations under Chapter IV with intent or as a result of gross negligence.

Amendment 90

Proposal for a directive
Article 18

Text proposed by the Commission	*Amendment*
Article 18	***deleted***
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.

Amendment 91

Proposal for a directive
Article 20 – paragraph 1

Text proposed by the Commission	*Amendment*
The Commission shall ***periodically*** review the functioning of this Directive and report to the European Parliament and the Council. The first report shall be submitted no later than ***three*** years after the date of transposition referred to in Article 21. For this purpose, the Commission may request Member States to provide information without undue delay.	The Commission shall ***every three years*** review the functioning of this Directive and report to the European Parliament and the Council. The first report shall be submitted no later than ***two*** 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.

Justification

To stay abreast of changing threats and conditions in the field of cyber security Annex II shall be reviewed and edited regularly.

Amendment 92

Proposal for a directive
Annex 1 – heading 1

Text proposed by the Commission	*Amendment*
Requirements and tasks of the Computer Emergency Response ***Team*** (CERT)	Requirements and tasks of the Computer Emergency Response ***Teams (CERTs)***

Amendment 93

Proposal for a directive
Annex 1 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
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:	The requirements and tasks of the ***CERTs*** shall be adequately and clearly defined and supported by national policy and/or regulation. They shall include the following elements: *(This amendment applies throughout the text of annex 1)*

Amendment 94

Proposal for a directive
Annex 1 – paragraph 1 – point 1 – point a

Text proposed by the Commission	*Amendment*
(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.	(a) The ***CERTs*** 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 ***at all times***. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.

Amendment 95

Proposal for a directive
Annex 1 – paragraph 1 – point 1 – point c

Text proposed by the Commission	*Amendment*
(c) The offices of the ***CERT*** and the supporting information systems shall be located in secure sites**.**	(c) The offices of the ***CERTs*** and the supporting information systems shall be located in secure sites ***with secured network information systems.***

Amendment 96

Proposal for a directive
Annex 1 – paragraph 1 – point 2 – point a – indent 1

Text proposed by the Commission	*Amendment*
– Monitoring incidents at a national level,	– ***Detection and*** monitoring incidents at a national level,

Amendment 97

Proposal for a directive
Annex 1 – paragraph 1 – point 2 – point a – indent 5 a (new)

Text proposed by the Commission	*Amendment*
	- Actively participate in Union and International CERT cooperation networks

Amendment 98

Proposal for a directive
Annex II

Text proposed by the Commission	*Amendment*
List of market operators	List of market operators
1. Energy	1. Energy
	(a) Electricity
	- Suppliers
	- Distribution system operators and retailers for final consumers
	- Transmission system operators in electricity
	- Electricity market operators
	(b) Oil
	- Oil transmission pipelines and oil storage
	- Operators of oil production, refining and

	treatment facilities, storage and transmission
	(c) Gas
	- Suppliers
	- Distribution system operators and retailers for final consumers
	- Natural gas transmission system operators, storage system operators and LNG system operators
	- Operators of natural gas production, refining, treatment facilities, storage facilities and transmission
	- Gas market operators
2. Transport	2. Transport
	(a) Road transport
	(i) Traffic management control operators
	(ii) Auxiliary logistics services:
	- warehousing and storage,
	- cargo handling, and
	- other transportation support activities
	(b) Rail transport
	(i) Railways (infrastructure managers, integrated companies and railway transport operators)
	(ii) Traffic management control operators
	(iii) Auxiliary logistics services:
	- warehousing and storage,
	- cargo handling, and
	- other transportation support activities
	(c) Air transport
	(i) Air carriers (freight and passenger air transport)
	(ii) Airports
	(iii) Traffic management control operators
	(iv) Auxiliary logistics services:

	- warehousing,
	- cargo handling, and
	- other transportation support activities
	(d) Maritime transport
	(i) Maritime carriers (inland, sea and coastal passenger water transport companies and inland, sea and coastal freight water transport companies)
	(ii) Ports
	(iii) Traffic management control operators
	(iv) Auxiliary logistics services:
	- warehousing and storage,
	- cargo handling, and
	- other transportation support activities
	2a. Water services
3. Banking: credit institutions in accordance with Article 4.1 of Directive 2006/48/CE.	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.	4. Financial market infrastructures: ***regulated markets, multilateral trading facilities, organised trading facilities, internet payment gateways*** and central counterparty clearing houses.
5. Health sector: health care settings (including hospitals and private clinics) and other entities involved in health care provisions.	5. Health sector: health care settings (including hospitals and private clinics) and other entities involved in health care provisions.
	6. ICT: Cloud computing services used by an operator to provide any of the services listed in point 1-5.
	This list shall be reviewed every 2 years.

PROCEDURE

Title	High common level of network and information security across the Union
References	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)
Committee responsible Date announced in plenary	IMCO 15.4.2013
Opinion by Date announced in plenary	ITRE 15.4.2013
Associated committee(s) - date announced in plenary	12.9.2013
Rapporteur Date appointed	Pilar del Castillo Vera 23.5.2013
Discussed in committee	14.10.2013 4.11.2013
Date adopted	16.12.2013
Result of final vote	+: 36 –: 5 0: 0
Members present for the final vote	Amelia Andersdotter, Josefa Andrés Barea, Bendt Bendtsen, Fabrizio Bertot, Reinhard Bütikofer, Maria Da Graça Carvalho, Giles Chichester, Pilar del Castillo Vera, Christian Ehler, Vicky Ford, Adam Gierek, Norbert Glante, Robert Goebbels, Fiona Hall, Romana Jordan, Philippe Lamberts, Marisa Matias, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Vittorio Prodi, Miloslav Ransdorf, Herbert Reul, Teresa Riera Madurell, Paul Rübig, Amalia Sartori, Salvador Sedó i Alabart, Evžen Tošenovský, Claude Turmes, Marita Ulvskog, Vladimir Urutchev
Substitute(s) present for the final vote	Daniel Caspary, António Fernando Correia de Campos, Françoise Grossetête, Roger Helmer, Jolanta Emilia Hibner, Seán Kelly, Eija-Riitta Korhola, Holger Krahmer, Zofija Mazej Kukovič, Silvia-Adriana Ţicău, Lambert van Nistelrooij
Substitute(s) under Rule 187(2) present for the final vote	María Auxiliadora Correa Zamora