



Council of the
European Union

Brussels, 4 November 2014

14850/14

**Interinstitutional File:
2013/0027 (COD)**

LIMITE

**TELECOM 189
DATAPROTECT 157
CYBER 55
MI 825
CSC 233
CODEC 2129**

NOTE

from: Presidency
to: Delegations

No. prev. doc.: 14669/14 TELECOM 185 DATAPROTECT 144 CYBER 53 MI 802 CSC 230
CODEC 2080

No. Cion prop.: 6342/13 TELECOM 24 DATAPRTOEC 14 CYBER 2 MI 104 CODEC 313

Subject: 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
- Preparations for the 2nd informal trilogue

1. On 10 October and on the basis of a number of main principles and general orientations set out in doc. 14076/14, the Coreper granted the Presidency a mandate to start informal exploratory talks with the EP on the above mentioned proposal. A first exploratory trilogue took place on 14 October and the Presidency informed the Coreper about the results of this event on 17 October.
2. In view of the second informal trilogue, which is planned to take place on 11 November, the Presidency now seeks an updated mandate to enter into more detailed discussions with the EP on the basis of a text, which is the result of detailed examination in the Council's WP TELE. This attached text is fully in line with the main principles and general orientations set out in doc. 14076/14, which still stand for the second informal trilogue.

3. As made clear in the 1st footnote in the ANNEX, the text inserted in the 3rd column of this 4-column document reflects the main views of the Member States expressed so far and should by no means be interpreted as the Council's final position on the proposal. The text in the 4th column gives a first indication of the Council's impression of EP's first reading amendments.
 4. The Presidency intends to debrief the WP TELE and the Coreper about the results achieved at the second informal trilogue at their respective meetings on Friday 14 November.
 5. Taking the above mentioned into account, the Presidency invites the Coreper to grant it an updated mandate to continue the talks with the EP on the basis of the text set out in ANNEX.
-

Proposal for a
Directive of the European Parliament and of the Council
concerning measures to ~~seek to achieve and maintain-ensure~~ a high common level of network and information security across the Union ¹

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
CHAPTER I		CHAPTER I	
GENERAL PROVISIONS		GENERAL PROVISIONS	
<i>Article 1</i>		<i>Article 1</i>	
Subject matter and scope		Subject matter and scope	
1. This Directive lays down measures to ensure a high common level of network and information security (hereinafter referred to as "NIS") within the Union.		1. This Directive lays down measures to <u>seek to achieve and maintain-ensure</u> a high common level of network and information security (hereinafter referred to as "NIS") within the Union <u>so as to improve the functioning of the internal market.</u>	
2. To that end, this Directive:		2. To that end, this Directive:	
(a) lays down obligations for all Member States concerning the prevention, the handling of and the response to risks and incidents affecting networks and information systems;		(a) lays down obligations for all Member States concerning the prevention, the handling of and the response to <u>serious</u> risks and incidents affecting networks and information systems;	

¹ Comment from the Council: the text inserted in the 3rd column of this 4-column document reflects the main views of the Member States expressed so far, which by no means should be interpreted as the Council's final position. The text in the 4th column gives a first indication of the Council's impression of EP's first reading amendments

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<p>(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;</p>	<p><u>AM40</u> (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, efficient <i>and effective</i> handling of and response to risks and incidents affecting network and information systems <i>with the participation of relevant stakeholders</i>;</p>	<p>(b) creates a cooperation <u>group mechanism</u> between Member States in order to <u>support and facilitate strategic cooperation and the exchange of information among Member States</u> 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;</p>	<p>Participation of stakeholders in the Coop. Group is covered in Art.8a</p>
		<p>(ba) creates a CSIRTs ("Computer Security Incident Response Team") <u>network in order to contribute to developing confidence and trust between Member States and to promote swift, effective operational cooperation;</u></p>	
<p>(c) establishes security requirements for market operators and public administrations.</p>	<p><u>AM41</u> (c) establishes security requirements for market operators.</p>	<p>(c) establishes security <u>and notification</u> requirements for market operators and public administrations.</p>	<p>"Operators" covers private and public entities referred to in Annex II, which provide essential services and fulfil specific criteria (see Article 3(8))</p>
		<p>(d) <u>lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs concerned with the security of network and information systems.</u></p>	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<p>3. The security requirements provided for in Article 14 shall apply neither to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC, which shall comply with the specific security and integrity requirements laid down in Articles 13a and 13b of that Directive, nor to trust service providers.</p>		<p>3. The security <u>and notification</u> requirements provided for in Article 14 shall apply neither to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC, which shall comply with the specific security and integrity requirements laid down in which are <u>subject to the requirements of</u> Articles 13a and 13b of that Directive <u>2002/21/EC</u>, nor to trust service providers <u>which are subject to the requirements of Article 19 of Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.</u></p>	
<p>4. This Directive shall be without prejudice to EU laws on cybercrime and Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection²</p>		<p>4. This Directive shall be without prejudice to EU laws on cybercrime and Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.³</p>	

² OJ L 345, 23.12.2008, p. 75.

³ OJ L 345, 23.12.2008, p. 75.

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<p>5. This Directive shall also be without prejudice to Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data⁴, and to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector and to the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data⁵.</p>	<p><u>AM42</u></p> <p>5. This Directive shall also be without prejudice to Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector and to the Regulation <i>(EC) No 45/2001</i> 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 <i>by the Community institutions and bodies</i> and on the free movement of such data. <i>Any use of the personal data shall be limited to what is strictly necessary for the purposes of this Directive, and those data shall be as anonymous as possible, if not completely anonymous.</i></p>	<p>5. This Directive shall also be without prejudice to Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data⁶, and to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [and to the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data].⁷.</p>	<p>Cion/EP to propose rewording/clarification</p> <p>As the issue of data protection appears in several places in the proposal, efforts should be made to address it in one place and in a consistent manner.</p>

⁴ OJ L 281 , 23/11/1995 p. 31.

⁵ SEC(2012) 72 final.

⁶ OJ L 281 , 23/11/1995 p. 31.

⁷ SEC(2012) 72 final.

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<p>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.</p>		<p>6. The sharing of information within the cooperation network under Chapter III and the notifications of NIS incidents under Article 14 may require <u>¶The processing of personal data necessary to meet the objectives of public interest pursued by this Directive, shall be authorised by the Member States pursuant to Article 7 of</u> be carried out in accordance with Directive 95/46/EC and Directive 2002/58//EC, as implemented in national law. <u>Such processing is a legitimate processing within the meaning of Article 7 of Directive 95/46/EC.</u></p>	
		<p>6a. <u>Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other competent authorities only where such exchange is necessary for the application of this Directive. The exchanged information shall be limited to that which is relevant and proportionate to the purpose of such exchange.</u></p>	<p>The exact wording of this new provision is still under consideration in the Council, in particular whether in 1(6a) or in a Recital, the following should be mentioned: "This Directive is without prejudice to the exercise of the responsibilities of the Member States with regard to national security, internal security and maintenance of law and order."</p>

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
		[7. If a sector specific Union legal act contains security and notification requirements covering network and information security, the provisions of that sector specific Union legal act shall apply instead of Article 14 of this Directive.]	The exact wording of this new provision is still under consideration in the Council.
	AM43 <i>Article 1a</i> <i>Protection and processing of personal data</i>		AM not yet discussed in Council. As the issue of data protection appears in several places in the proposal, efforts should be made to address it in one place and in a consistent manner.
	<i>1. Any processing of personal data in the Member States pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC and Directive 2002/58/EC.</i>		
	<i>2. Any processing of personal data by the Commission and ENISA pursuant to this Regulation shall be carried out in accordance with Regulation (EC) No 45/2001.</i>		
	<i>3. Any processing of personal data by the European Cybercrime Centre within Europol for the purposes of this Directive shall be carried out pursuant to Decision 2009/371/JHA.</i>		

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	<p><i>4. The processing of personal data shall be fair and lawful and strictly limited to the minimum data needed for the purposes for which they are processed. They shall be kept in a form which permits the identification of data subjects for no longer than necessary for the purpose for which the personal data are processed.</i></p>		
	<p><i>5. Incident notifications referred to in Article 14 shall be without prejudice to the provisions and obligations regarding personal data breach notifications set out in Article 4 of Directive 2002/58/EC and in Regulation (EU) No 611/2013.</i></p>		

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<i>Article 2</i>		<i>Article 2</i>	
Minimum harmonisation		Minimum harmonisation	
Member States shall not be prevented from adopting or maintaining provisions ensuring a higher level of security, without prejudice to their obligations under Union law.		Member States shall not be prevented from adopting or maintaining provisions <u>seeking to achieve and maintain</u> ensuring a higher level of <u>network and information</u> security, without prejudice to their obligations under Union law.	
<i>Article 3</i>	<i>Article 3</i>	<i>Article 3</i>	
Definitions	Definitions	Definitions	
For the purpose of this Directive, the following definitions shall apply:		For the purpose of this Directive, the following definitions shall apply:	
(1) "network and information system" means:		(1) "network and information system" means:	
(a) an electronic communications network within the meaning of Directive 2002/21/EC, and		(a) an electronic communications network within the meaning of <u>point (a) of Article 2 of Directive 2002/21/EC</u> , and	
(b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of computer data, as well as	<u>AM44</u> (b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data, as well as	(b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of computer data, as well as	Possibly acceptable
(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.	<u>AM45</u> (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.	(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.	Possibly acceptable

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
(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;	<u>AM46</u> (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; <i>'security' includes appropriate technical devices, solutions and operating procedures ensuring the security requirements set out in this Directive.</i>	(2) " <u>network and information security</u> " means the ability of a network and information system to resist, at a given level of confidence, <u>any accident or malicious</u> action that compromise the availability, authenticity, integrity <u>or</u> and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system;	Not yet discussed in Council. Not clear what the AM would add to the substantive provisions of the proposal
		(2a) " <u>essential services</u> " means <u>services essential for the maintenance of critical societal and economic activities.</u>	
(3) "risk" means any circumstance or event having a potential adverse effect on security;	<u>AM47</u> (3) 'risk' means any <i>reasonably identifiable</i> circumstance or event having a potential adverse effect on security;	(3) "risk" means any circumstance or event having a potential <u>serious or actual</u> adverse effect on <u>network and information</u> security;	The drafting of this definition requires further clarification
(4) "incident" means any circumstance or event having an actual adverse effect on security;	<u>AM48</u> (4) 'incident' means any event having an actual adverse effect on security;	(4) "incident" means any circumstance or event having an actual adverse effect on <u>network and information</u> security;	Possibly acceptable subject to consistency check with AM 53
(5) "information society service" mean service within the meaning of point (2) of Article 1 of Directive 98/34/EC;	<u>AM49</u> <i>deleted</i>	deleted	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
(6) "NIS cooperation plan" means a plan establishing the framework for organisational roles, responsibilities and procedures to maintain or restore the operation of networks and information systems, in the event of a risk or an incident affecting them;		deleted	
		(6a) "National NIS strategy" means a <u>framework providing high-level vision, objectives and priorities on NIS at national level;</u>	
(7) "incident handling" means all procedures supporting the analysis, containment and response to an incident;	<u>AM50</u> (7) 'incident handling' means all procedures supporting the <i>detection, prevention,</i> analysis, containment and response to an incident;	(7) "incident handling" means all procedures supporting the analysis, containment and response to an incident;	Possibly partly acceptable
(8) "market operator" means:		(8) "market operator" means:	
(a) provider of information society services which enable the provision of other information society services, a non exhaustive list of which is set out in Annex II;	<u>AM51</u> <i>deleted</i>	deleted	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<p>(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.</p>	<p><u>AM52</u> (b) operator of infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, <i>financial market infrastructures, internet exchange points, food supply chain</i> and health, <i>and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions</i>, a non exhaustive list of which is set out in Annex II, <i>insofar as the network and information systems concerned are related to its core services;</i></p>	<p>(b) operator <u>means a public or private entity referred to in Annex II, which provides an essential service in the fields of critical digital Internet infrastructure and service platforms, that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health, and water supply and which fulfills all of the following criteria</u> a non exhaustive list of which is set out in Annex II.</p>	<p>The thrust of the AM has been taken on board in the Council definition of "operator". This definition is still under consideration in the Council</p>
		<p><u>- the service depends heavily on network and information systems;</u></p>	
		<p><u>- an incident to the network and information systems of the service having serious disruptive effects on the provision of that essential service or on public safety.</u></p>	
		<p><u>[In addition to the above criteria, entities in the field of service platforms shall also fulfil the criterion that a large number of market participants rely on the entity for their trading/economic activities.]</u></p>	<p>Bracketed because still under consideration in the Council</p>
		<p><u>Each Member State shall identify on its territory entities, which meet the above definition of operator.</u></p>	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	<u>AM53</u> <i>(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;</i>		The thrust of the AM is taken on board in the Council's proposed definitions (2a) and (4) but could be discussed further.
(9) "standard" means a standard referred to in Regulation (EU) No 1025/2012;		(9) "standard" means a standard referred to in <u>point (1) of Article 2</u> of Regulation (EU) No 1025/2012;	
(10) "specification" means a specification referred to in Regulation (EU) No 1025/2012;		(10) "specification" means a <u>technical</u> specification referred to in <u>point (4) of Article 2</u> of Regulation (EU) No 1025/2012;	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<p>(11) "Trust service provider" means a natural or legal person who provides any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals.</p>		<p>(11) "Trust service provider" means a natural or legal person <u>within the meaning of point (19) of Article 3 of Regulation 910/2014</u> who provides any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals.</p>	
	<p><u>AM54</u> <i>(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^{1a};</i></p> <p>----- ^{1a} <i>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).</i></p>		<p>To be considered further in conjunction with Annex II.</p>
	<p><u>AM55</u> <i>(11b) 'multilateral trading facility (MTF)' means multilateral trading facility as defined in point 15 of Article 4 of Directive 2004/39/EC;</i></p>		<p>To be considered further in conjunction with Annex II.</p>

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	<p><u>AM56</u> <i>(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 such a way as to result in a contract in accordance with Title II of Directive 2004/39/EC;</i></p>		To be considered further in conjunction with Annex II.
CHAPTER II	CHAPTER II	CHAPTER II	
NATIONAL FRAMEWORKS ON NETWORK AND INFORMATION SECURITY	NATIONAL FRAMEWORKS ON NETWORK AND INFORMATION SECURITY	NATIONAL FRAMEWORKS ON NETWORK AND INFORMATION SECURITY	
<i>Article 4</i>		<i>Article 4</i>	
Principle		Principle	
Member States shall ensure a high level of security of the network and information systems in their territories in accordance with this Directive.		deleted	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<i>Article 5</i>	<i>Article 5</i>	<i>Article 5</i>	
National NIS strategy and national NIS cooperation plan	National NIS strategy and national NIS cooperation plan	National NIS strategy and national NIS cooperation plan	
1. Each Member State shall adopt a national NIS strategy defining the strategic objectives and concrete policy and regulatory measures to achieve and maintain a high level of network and information security. The national NIS strategy shall address in particular the following issues:		1. Each Member State shall adopt a national NIS strategy defining the strategic objectives and concrete policy and regulatory measures to <u>seek to</u> achieve and maintain a high level of network and information security [] <u>at least in the fields referred to in Article 3(8)</u> . The national NIS strategy shall address in particular the following issues:	The last part of the first sentence of this paragraph is still under consideration in the Council
(a) The definition of the objectives and priorities of the strategy based on an up-to-date risk and incident analysis;		(a) The definition of the <u>The</u> objectives and priorities <u>of the national NIS strategy based on an up to date risk and incident analysis;</u>	
(b) A governance framework to achieve the strategy objectives and priorities, including a clear definition of the roles and responsibilities of the government bodies and the other relevant actors;		[(b) <u>The</u> A governance framework <u>put in place</u> to achieve the strategy objectives and priorities <u>of the national NIS strategy, including a clear definition of the roles and responsibilities of the government bodies and the other relevant actors;</u>]	
(c) The identification of the general measures on preparedness, response and recovery, including cooperation mechanisms between the public and private sectors;		(c) The identification of the general measures on preparedness, response and recovery [, including cooperation mechanisms between the public and private sectors];	
(d) An indication of the education, awareness raising and training programmes;		(d) An indication of the education, awareness raising and training programmes <u>relating to the NIS strategy;</u>	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
(e) Research and development plans and a description of how these plans reflect the identified priorities.		(e) — Research and development plans and a description of how these plans reflect the identified priorities.	
	<u>AM57</u> <i>(ea) Member States may request the assistance of ENISA in developing their national NIS strategies and national NIS cooperation plans, based on a common minimum NIS strategy.</i>		Possibly partly acceptable.
2. The national NIS strategy shall include a national NIS cooperation plan complying at least with the following requirements		deleted	
(a) A risk assessment plan to identify risks and assess the impacts of potential incidents;	<u>AM58</u> <i>(a) A risk management framework to establish a methodology for the identification, prioritisation, evaluation and treatment of risks, the assessment of the impacts of potential incidents, prevention and control options, and to define criteria for the choice of possible countermeasures;</i>	(f) A risk assessment plan to identify potential risks and assess the impacts of potential incidents;	Too prescriptive
(b) The definition of the roles and responsibilities of the various actors involved in the implementation of the plan;	<u>AM59</u> <i>(b) The definition of the roles and responsibilities of the various authorities and other actors involved in the implementation of the framework;</i>	(g) The definition of the roles and responsibilities <u>A list</u> of the various actors involved in the implementation of the <u>NIS strategy plan;</u>	Council calls it "NIS strategy", not "framework". Possibly ok to insert "authorities and other"

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
(c) The definition of cooperation and communication processes ensuring prevention, detection, response, repair and recovery, and modulated according to the alert level;		deleted	
(d) A roadmap for NIS exercises and training to reinforce, validate, and test the plan. Lessons learned to be documented and incorporated into updates to the plan.		deleted	
3. The national NIS strategy and the national NIS cooperation plan shall be communicated to the Commission within one month from their adoption.	<u>AM60</u> 3. The national NIS strategy and the national NIS cooperation plan shall be communicated to the Commission within <i>three months</i> from their adoption.	3. The <u>Member States shall make available to the Commission at least a summary of the national NIS strategy</u> and the national NIS cooperation plan shall be communicated to the Commission within one month from their adoption.	Possibly not acceptable

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
Article 6	Article 6	Article 6	
National competent authority on the security of network and information systems	<u>AM61</u> National competent <i>authorities and single points of contact</i> on the security of network and information systems	National competent <u>authorities</u> and <u>single point of contact on the security of network and information systems</u>	Council text is simpler
1. Each Member State shall designate a national competent authority on the security of network and information systems (the "competent authority").	<u>AM62</u> 1. Each Member State shall designate <i>one or more civilian</i> national competent <i>authorities</i> on the security of network and information systems (<i>hereinafter referred to as 'competent authority/ies'</i>).	1. Each Member State shall designate <u>one or more a</u> national competent <u>authorities</u> on the security of network and information systems (the "competent authority"). <u>Member States may designate this role to an existing authority or authorities.</u>	The thrust of the AM has been taken on board in the Council text (without the insertion of "civilian", however)
2. The competent authorities shall monitor the application of this Directive at national level and contribute to its consistent application throughout the Union		deleted	
	<u>AM63</u> <i>2a. Where a Member State designates more than one competent authority, it shall designate a civilian 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.</i>	<u>2a. Member States shall designate a national single point of contact on network and information security ('single point of contact'). Member States may designate this role to an existing authority.</u>	EP and Council agree that MS should designate one SPC. Although strictly speaking not necessary, last part of the AM possibly acceptable

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	<u>AM64</u> 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.	<u>[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.]</u>	Possibly acceptable but really necessary? Therefore in [brackets] for the time being. Also: overlap with article 7(1a)?
	<u>AM65</u> 2c. The single point of contact shall ensure cross-border cooperation with other single points of contact.		The tasks of the SPC need further clarification, also in regard of their link with and role in the Coop. Group and with the SPCs of other MS
<p>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.</p>	<u>AM66</u> <p>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.</p>	<p>[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 group referred to in Article 8a.]</p>	Similar comment as for AM65. Also: allocation of resources is a MS responsibility.

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<p>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.</p>	<p><u>AM67</u> 4. Member States shall ensure that the competent authorities <i>and single points of contact, where applicable in accordance with paragraph 2a of this Article</i>, 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.</p>	<p>deleted</p>	
	<p><u>AM68</u> <i>4a. Where Union law provides for a sector-specific Union supervisory or regulatory body, inter alia on the security of network and information systems, that body shall receive the notifications of incidents in accordance with Article 14(2) from the market operators concerned in that sector and be granted the implementation and enforcement powers referred to under Article 15. That Union body shall cooperate closely with the competent authorities and the single point of contact of the host Member State with regard to those obligations. The single point of contact of the host Member State shall represent the Union body with regard to the obligations laid down in Chapter III.</i></p>		<p>Possibly not acceptable as far too prescriptive</p>

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
5. The competent authorities shall consult and cooperate, whenever appropriate, with the relevant law enforcement national authorities and data protection authorities.	<u>AM69</u> 5. The competent authorities <i>and single points of contact</i> shall consult and cooperate, whenever appropriate, with the relevant law enforcement national authorities and data protection authorities.	5. The competent authorities shall consult and cooperate, whenever appropriate <u>and in accordance with national legislation</u> , with the relevant [law enforcement national authorities and data protection] authorities.	Possibly not acceptable
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.	<u>AM70</u> 6. Each Member State shall notify to the Commission without delay the designation of the competent <i>authorities and the single point of contact</i> , its tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent <i>authorities</i> .	6. Each Member State shall notify to the Commission without delay the designation of the competent authorities <u>and single point of contact</u> , their its tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent authorities <u>and single point of contact</u> .	Reflected in Council text
<i>Article 7</i>	<i>Article 7</i>	<i>Article 7</i>	
Computer Emergency Response Team	Computer Emergency Response Team	Computer <u>Security Incident</u> Emergency Response Teams	
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.	<u>AM71</u> 1. Each Member State shall set up <i>at least one</i> Computer Emergency Response Team (hereinafter: 'CERT') <i>for each of the sectors established in Annex II</i> , 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 <u>designate one or more</u> set up a Computer <u>Security Incident</u> Emergency Response Teams (hereinafter: " <u>CSIRTs</u> CERTs ") 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 <u>CSIRT</u> may be established within the competent authority.	Partly taken on board

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
		<p><u>1a. Where they are separate, the competent authorities, the single point of contact and the CSIRTs CERTs of the same Member State [shall] cooperate with regard to the obligations laid down in this Directive. To the extent necessary to fulfil its tasks, CSIRTS shall be granted access to data on incidents notified by operators pursuant to Article 14(2).</u></p>	
<p>2. Member States shall ensure that CERTs have adequate technical, financial and human resources to effectively carry out their tasks set out in point (2) of Annex I.</p>		<p>[2. Member States shall ensure that <u>CSIRTS</u> CERTs have adequate technical, financial and human resources to effectively carry out their tasks set out in point (2) of Annex I.]</p>	
<p>3. Member States shall ensure that CERTs rely on a secure and resilient communication and information infrastructure at national level, which shall be compatible and interoperable with the secure information-sharing system referred to in Article 9.</p>		<p>3. Member States shall ensure that <u>CSIRTS</u> CERTs <u>have access to an appropriate</u> rely on a secure and resilient communication and information infrastructure at national level, which shall be compatible and interoperable with the secure information-sharing system referred to in Article 9.</p>	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
4. Member States shall inform the Commission about the resources and mandate as well as the incident handling process of the CERTs.		4. Member States shall inform the Commission about the <u>remit</u> resources and mandate as well as the incident handling process of the <u>CSIRTs</u> CERTs.	
5. The CERT shall act under the supervision of the competent authority, which shall regularly review the adequacy of its resources, its mandate and the effectiveness of its incident-handling process.	<u>AM72</u> 5. The CERTs shall act under the supervision of the competent authority or the single point of contact , which shall regularly review the adequacy of their resources, mandates and the effectiveness of their incident-handling process.	deleted	See article 8a(3a): the Cooperation Group shall guide the CSIRTs network

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	<u>AM73</u> <i>5a. Member States shall ensure that CERTs have adequate human and financial resources to actively participate in international, and in particular Union, cooperation networks</i>		Possibly not acceptable or possibly to be covered under paragraph 2 above
	<u>AM74</u> <i>5b 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.</i>		Not yet discussed in Council. To be cross-checked against ENISA's tasks
	<u>AM75</u> <i>5c. Member States may ask for the assistance of ENISA or of other Member States in developing their national CERTs.</i>		Possibly acceptable. Not yet discussed in Council. To be cross-checked against ENISA's tasks

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
CHAPTER III	CHAPTER III	CHAPTER III	
COOPERATION BETWEEN COMPETENT AUTHORITIES	COOPERATION BETWEEN COMPETENT AUTHORITIES	COOPERATION BETWEEN MEMBER STATES COMPETENT AUTHORITIES AND CSIRTs <u>CERTs</u>	
<i>Article 8</i>	<i>Article 8</i>	<i>Article 8</i>	
Cooperation network	Cooperation network	Cooperation network	
1. The competent authorities and the Commission shall form a network ("cooperation network") to cooperate against risks and incidents affecting network and information systems.	<u>AM76</u> 1. The <i>single points of contact</i> and the Commission <i>and ENISA</i> shall form a network (<i>hereinafter referred to as 'cooperation network'</i>) to cooperate against risks and incidents affecting network and information systems.	<u>Replaced by article 8a</u>	OK to include ENISA but MS to determine whom to send to the Coop.Gr.
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.	<u>AM77</u> 2. The cooperation network shall bring into permanent communication the Commission and the <i>single points of contact</i> . When requested, ENISA shall assist the cooperation network by providing its expertise and advice. <i>Where appropriate, market operators and suppliers of cyber security solutions may also be invited to participate in the activities of the cooperation network referred to in points (g) and (i) of paragraph 3. Where relevant, the cooperation network shall cooperate with the data protection authorities. The Commission shall regularly inform the cooperation network of security research and other relevant programmes of Horizon2020.</i>	<u>Replaced by article 8a</u>	Partly covered in Council's new text for article 8a(2)

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
3. Within the cooperation network the competent authorities shall:	<u>AM78</u> 3. Within the cooperation network the <i>single points of contact</i> shall:	<u>Replaced by article 8a</u>	Not yet discussed in Council. In particular EP's text on paragraphs (f), (fa), (ia) & (ib) needs further consideration
(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;	<u>Replaced by article 8a</u>	
(b) ensure a coordinated response in accordance with Article 11;	(b) ensure a coordinated response in accordance with Article 11;	<u>Replaced by article 8a</u>	
(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;	<u>Replaced by article 8a</u>	
(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;	<u>Replaced by article 8a</u>	
(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 the effectiveness of the CERTs, in particular when NIS exercises are performed at Union level;	<u>Replaced by article 8a</u>	
(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;	<u>AM78 (cont'd)</u> (f) cooperate and exchange <i>expertise on relevant matters on network and information security</i> , in particular in the fields of data protection, energy, transport, banking, <i>financial markets</i> and health <i>with the European Cybercrime Centre within Europol, and with other relevant European bodies</i> ;	<u>Replaced by article 8a</u>	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	<u>AM78 (cont'd)</u> <i>(fa) where appropriate, inform the EU Counter-terrorism Coordinator, by means of reporting, and may ask for assistance for analysis, preparatory works and actions of the cooperation network;</i>		
(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;	<u>Replaced by article 8a</u>	
(h) organise regular peer reviews on capabilities and preparedness;		<u>Replaced by article 8a</u>	
(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.	<u>Replaced by article 8a</u>	
	<u>AM78 (cont'd)</u> <i>(ia) involve, consult and exchange, where appropriate, information with market operators with respect to the risks and incidents affecting their network and information systems;</i>		
	<u>AM78 (cont'd)</u> <i>(ib) develop, in cooperation with ENISA, guidelines for sector-specific criteria for the notification of significant incidents, in addition to the parameters laid down in Article 14(2), for a common interpretation, consistent application and harmonious implementation within the Union.</i>		

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	<u>AM79</u> <i>3a. The cooperation network shall publish a report once a year, 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.</i>		To be compared with Council's newly proposed article 8a(4)
		<i>Article 8a</i>	
		Cooperation group network	
		<u>1. In order to support and facilitate strategic cooperation and the exchange of information among Member States, a cooperation group is hereby established.</u>	
		<u>2. The cooperation group shall be composed of representatives from the Member States, the Commission and the European Network and Information Security Agency (“ENISA”). The Commission shall provide the secretariat. The Group may invite representatives from the relevant stakeholders to participate in its meetings.</u>	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
		<u>3. The tasks of the cooperation group shall be to:</u>	
		<u>a. Provide guidance for the activities of the CSIRTs network established under Article 8b.</u>	
		<u>ab. Exchange best practice on the exchange of information related to incident notification referred to in Article 14(2b).⁸</u>	
		<u>b. Exchange best practices between Member States and, in collaboration with ENISA, assist Member States in building capacity in NIS;⁹</u>	
		<u>c. At the request of a Member State organise regular peer reviews on capabilities and preparedness of that same Member State;¹⁰</u>	
		<u>d. At the request of a Member State discuss the national NIS strategy of that same Member State;¹¹</u>	
		<u>e. At the request of a Member State discuss the effectiveness of the CSIRT of that same Member State.¹²</u>	

⁸ This provisions corresponds to Article 8(3)a in the Commission's proposal.

⁹ This provisions corresponds to Article 8(3)g in the Commission's proposal.

¹⁰ This provisions corresponds to Article 8(3)h in the Commission's proposal.

¹¹ This provisions corresponds to Article 8(3)d in the Commission's proposal.

¹² This provisions corresponds to Article 8(3)e in the Commission's proposal.

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
		<u>f. Exchange information and best practice on awareness raising and training.</u>	
		<u>g. Exchange information and best practice on research and development on network and information security.</u>	
		<u>h. With representatives from the relevant European Standards Organisations, discuss the standards referred to in Article 16.</u>	
		<u>i. Collect best practice information on risks and incidents affecting network and information systems and, where appropriate, exchange relevant unrestricted information with operators with respect to the risks and incidents affecting their network and information systems;</u>	
		<u>j. In collaboration with ENISA, agree a roadmap for NIS exercises, education programmes and training.</u>	
		<u>k. With ENISA's assistance, exchange best practices with regard to the identification of operators by the Member States.</u>	
		<u>l. Discuss cross-border dependencies regarding NIS risks and incidents</u>	
		<u>4. As input to the Commission's periodic review of the functioning of this Directive, the cooperation group shall produce a report on the experience gained with the strategic cooperation pursued under this Directive.</u>	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<p>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).</p>	<p><u>AM80</u> 4. The Commission shall establish, by means of implementing acts, the necessary modalities to facilitate the cooperation between <i>single points of contact</i>, the Commission <i>and ENISA</i> referred to in paragraphs 2 and 3. Those implementing acts shall be adopted in accordance with the <i>examination</i> procedure referred to in Article 19(3).</p>	<p>4. The Commission shall <u>establish</u>, by means of implementing acts, <u>procedural arrangements necessary for the functioning of the Cooperation Group</u>. 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).</p>	<p>Possibly not acceptable. Council could poss. only support implementing acts on procedural arrangements, not on cooperation/substance</p>
		<u>Article 8b</u>	
		<u>CSIRTs network</u>	
		<p><u>1. In order to contribute to developing confidence and trust between the Member States and to promote swift, effective operational, a network of the national CSIRTs is hereby established.</u></p>	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
		<p><u>2. The CSIRTs network shall be composed of representatives from the national CSIRTs and from the CERT-EU. The [Commission and the European Network and Information Security Agency (ENISA) shall participate in the CSIRTs network as observers. ENISA shall provide secretariat functions.</u></p>	
		<p><u>3. The CSIRTs network shall have the following tasks:</u></p>	
		<p><u>a. Exchange high-level information on CSIRTs services, operations and cooperation capabilities.</u></p>	
		<p><u>b. At the request of any Member State, exchange and discuss non-commercially sensitive information related to risks and on-going incidents. This request may be refused if the Member State dealing with the incident deems that it is inappropriate to share information for reasons directly relating to the operational response to the incident or its investigation, in which case the Member State in question shall only disclose the minimum information necessary to alert the CSIRT network on possible risks.</u></p>	
		<p><u>c. Exchange and publish on a voluntary basis anonymised information on incidents, which occurred in the past.</u></p>	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
		<u>d. At the request of a Member State discuss and, where possible, identify a coordinated response to an incident that has been identified within the jurisdiction of that same Member State.</u>	
		<u>e. Assist each other in cross-border incidents on the basis of voluntary mutual assistance.</u>	
		<u>f. Explore further forms of operational cooperation, such as voluntary mechanisms for cross-border alerts and for mutual assistance.</u>	
		<u>g. Inform the Cooperation Group on its activities and on the further forms of operational cooperation discussed pursuant to paragraph 3a, and request guidance related thereto.</u>	
		<u>8b(3a) The CERTs network shall discuss further forms of operational cooperation, including as regards:</u>	
		<u>(1) categories of risks and incidents, which could be subject to further operational cooperation;</u>	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
		<u>(2) early warnings, the criteria for their use and modalities for their circulation;</u>	
		<u>(3) mutual assistance for prevention, detection, mitigation, response and recovery on actual risks and incidents.</u>	
		<u>8b(3b) In order to facilitate the convergence of (operational) practices with regard to the application of the provisions of this Directive concerning operational cooperation, the CSIRTs network may issue guidelines.</u>	
		<u>4. As input to the Commission's periodic review of the functioning of this Directive, the CSIRTs network shall produce a report on the experience gained with the operational cooperation pursued under this Directive.</u>	
		<u>5. The CSIRTs network shall define its own rules of procedure.</u>	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<i>Article 9</i>	<i>Article 9</i>	<i>Article 9</i>	
Secure information-sharing system	Secure information-sharing system	Secure information-sharing system	
1. The exchange of sensitive and confidential information within the cooperation network shall take place through a secure infrastructure.		deleted	
	<u>AM81</u> <i>1a. Participants to the secure infrastructure shall comply with, inter alia, appropriate confidentiality and security measures in accordance with Directive 95/46/EC and Regulation (EC) No 45/2001 at all steps of the processing.</i>		Council deleted art.9
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:	<u>AM82</u> deleted	deleted	Council deleted art.9
(a) the availability of a secure and resilient communication and information infrastructure at national level, compatible and interoperable with the secure infrastructure of the cooperation network in compliance with Article 7(3), and		deleted	Council deleted art.9

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
(b) the existence of adequate technical, financial and human resources and processes for their competent authority and CERT allowing an effective, efficient and secure participation in the secure information-sharing system under Article 6(3), Article 7(2) and Article 7(3).		deleted	Council deleted art.9
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).	<u>AM83</u> 3. The Commission shall adopt, by means of <i>delegated acts, a common set of interconnection and security standards that single points of contact are to meet before exchanging sensitive and confidential information across the cooperation network.</i>	deleted	Council deleted art.9
Article 10	Article 10	Article 10	Council deleted art.10
Early warnings	Early warnings	Early warnings ¹³	
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:	<u>AM84</u> 1. The <i>single points of contact</i> 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:	deleted	Council deleted art.10 but included the principle of early warning in art.14. AM not yet discussed in Council. The Comp. Auth. rather than the SPC shall do the assessment referred to in (b).
(a) they grow rapidly or may grow rapidly in scale;		deleted	
(b) they exceed or may exceed national response capacity;	(b) <i>the single point of contact assesses that the risk or incident potentially exceeds</i> national response capacity;	deleted	

¹³ EP AMs related to "early warnings" are relevant to the Council's text in regard of Article 14.

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
(c) they affect or may affect more than one Member State.	(c) <i>the single points of contact or the Commission assess that the risk or incident affects</i> more than one Member State.	deleted	
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.	<u>AM85</u> 2. In the early warnings, the <i>single points of contact</i> and the Commission shall communicate <i>without undue delay</i> any relevant information in their possession that may be useful for assessing the risk or incident.	deleted	Council deleted art.10. AM not yet discussed in Council.
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.	<u>AM86</u> <i>deleted</i>	deleted	Council deleted art.10. AM not yet discussed in Council.
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.	<u>AM87</u> <i>deleted</i>	deleted	
	<u>AM88</u> <i>4a. Members of the cooperation network shall not make public any information received on risks and incidents referred to in paragraph 1 without having received the prior approval of the notifying single point of contact.</i>		Council deleted art.10. AM not yet discussed in Council.

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	<i>Furthermore, prior to sharing information in the cooperation network, the notifying single point of contact shall inform the market operator to which the information relates of its intention, and where it considers this appropriate, it shall make the information concerned anonymous.</i>		
	<u>AM89</u> <i>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.</i>		Council deleted art.10. AM not yet discussed in Council. To be cross-checked against ENISA's tasks
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.		deleted	
<i>Article 11</i>	<i>Article 11</i>	<i>Article 11</i>	Council deleted art.11
Coordinated response	Coordinated response	Coordinated response	
1. Following an early warning referred to in Article 10 the competent authorities shall, after assessing the relevant information, agree on a coordinated response in accordance with the Union NIS cooperation plan referred to in Article 12.	<u>AM90</u> 1. Following an early warning referred to in Article 10 the <i>single points of contact</i> shall, after assessing the relevant information, agree <i>without undue delay</i> on a coordinated response in accordance with the Union NIS cooperation plan referred to in Article 12.	deleted	Possibly not acceptable. The Comp. Auth. rather than the SPC shall do the assessment

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
2. The various measures adopted at national level as a result of the coordinated response shall be communicated to the cooperation network.		deleted	
<i>Article 12</i>	<i>Article 12</i>	<i>Article 12</i>	Council deleted art.12
Union NIS cooperation plan	Union NIS cooperation plan	Union NIS cooperation plan	
1. The Commission shall be empowered to adopt, by means of implementing acts, a Union NIS cooperation plan. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).		deleted	
2. The Union NIS cooperation plan shall provide for:		deleted	
(a) for the purposes of Article 10:		deleted	
– 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,	<u>AM91</u> – a definition of the format and procedures for the collection and sharing of compatible and comparable information on risks and incidents by the <i>single points of contact</i> ,		Possibly not acceptable
– a definition of the procedures and the criteria for the assessment of the risks and incidents by the cooperation network.		deleted	
(b) the processes to be followed for the coordinated responses under Article 11, including identification of roles and responsibilities and cooperation procedures;		deleted	
(c) a roadmap for NIS exercises and training to reinforce, validate, and test the plan;		deleted	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
(d) a programme for transfer of knowledge between the Member States in relation to capacity building and peer learning;		deleted	
(e) a programme for awareness raising and training between the Member States.		deleted	
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.	<u>AM92</u> 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. <i>The results of each revision shall be reported to the European Parliament.</i>	deleted	Possibly not acceptable
	<u>AM93</u> <i>3a. Coherence between the Union NIS cooperation plan and national NIS strategies and cooperation plans, as provided for in Article 5 of this Directive, shall be ensured.</i>		Possibly partly acceptable

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<i>Article 13</i>	<i>Article 13</i>	<i>Article 13</i>	
International cooperation	International cooperation	International cooperation	
<p>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.</p>	<p><u>AM94</u></p> <p>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 <i>and shall set out the monitoring procedure that must be followed to guarantee the protection of such personal data. The European Parliament shall be informed about the negotiation of the agreements. 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.</i></p>	<p>[Without prejudice to the possibility for the cooperation network to have informal international cooperation, the Union may conclude international agreements <u>in accordance with Article 218 TFEU</u> with third countries or international organisations allowing and organizing their participation in some activities of the cooperation <u>group network</u>. Such agreement shall take into account the need to ensure adequate protection of <u>sensitive data</u>, <u>including the</u> personal data circulating <u>within</u> on the cooperation <u>group network</u>.]</p>	<p>Still under consideration in the Council. AM not yet discussed</p>

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	<u>AM95</u> <i>Article 13a</i> <i>Level of criticality of market operators</i>		The thrust of the AM is taken on board in the Council's text of Article 3(2a), 3(8)
	<i>Member States may determine the level of criticality of market operators, taking into account the specificities of sectors, parameters including the importance of the particular market operator for maintaining a sufficient level of the sectoral service, the number of parties supplied by the market operator, and the time period until the discontinuity of the core services of the market operator has a negative impact on the maintenance of vital economic and societal activities.</i>		

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
CHAPTER IV		CHAPTER IV	
SECURITY OF THE NETWORKS AND INFORMATION SYSTEMS OF PUBLIC ADMINISTRATIONS AND MARKET OPERATORS		SECURITY OF THE NETWORKS AND INFORMATION SYSTEMS OF PUBLIC ADMINISTRATIONS AND MARKET OPERATORS	
<i>Article 14</i>	<i>Article 14</i>	<i>Article 14</i>	
Security requirements and incident notification	Security requirements and incident notification	Security requirements and incident notification	
<p>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.</p>	<p><u>AM96</u></p> <p>1. Member States shall ensure that market operators take appropriate <i>and proportionate</i> technical and organisational measures to <i>detect and effectively</i> 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, <i>those</i> measures shall <i>ensure</i> a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting <i>the security of</i> their network and information <i>systems</i> on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.</p>	<p>1. Member States shall <u>require ensure</u> that market operators and public administrations take appropriate <u>and proportionate, sector-specific</u> technical and organisational measures to manage the risks posed to the security of the <u>networks and information security of</u> systems which they control and use in their operations. Having regard to the state of the art, these measures shall <u>maintain</u> guarantee a level of <u>network and information</u> security appropriate to the risk presented.</p>	<p>Possibly acceptable with the exception of "ensuring" security</p>

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
		<u>1a</u> In particular, Member States shall require that operators take appropriate measures shall be taken to prevent and minimise the impact of incidents affecting their network and information security system on of the essential 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.	<u>AM97</u> 2. Member States shall ensure that market operators notify <i>without undue delay</i> to the competent authority <i>or to the single point of contact</i> incidents having a significant impact on the <i>continuity</i> of the core services they provide. <i>Notification shall not expose the notifying party to increased liability.</i>	2. Member States shall <u>provide for a reporting scheme pursuant to which ensure that market operators and public administrations shall notify without undue delay</u> to the competent authority incidents having a significant impact on the <u>continuity security</u> of the essential core services they provide.	Possibly partly acceptable
	<i>To determine the significance of the impact of an incident, the following parameters shall inter alia be taken into account:</i>	<u>2a</u> <u>To determine the significance of the impact of an incident, the following parameters in particular shall be taken into account:</u>	Included in the Council text for the time being but still subject to further consideration
	<u>AM98</u> <i>(a) the number of users whose core service is affected;</i>	<u>a) the number of users affected by the disruption of the essential service;</u>	Included in the Council text for the time being but still subject to further consideration
	<u>AM99</u> <i>(b) the duration of the incident;</i>	<u>(b) the duration of the incident;</u>	Included in the Council text for the time being but still subject to further consideration

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	<u>AM100</u> <i>(c) geographic spread with regard to the area affected by the incident.</i>	<u>(c) the geographical spread with regard to the area affected by the incident.</u> ¹⁴	Included in the Council text for the time being but still subject to further consideration
	<u>AM101</u> <i>Those parameters shall be further specified in accordance with point (ib) of Article 8(3).</i>		Not yet discussed in Council. Discussion on determining the "significance" of incidents still ongoing
	<u>AM102</u> <i>2a. Market operators shall 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.</i>	<u>2b When notifying an incident to its national competent authority, an operator shall include relevant information allowing the competent authority to determine the cross-border effect of that incident. Based on the information provided by the operator, the competent authority or the single point of contact shall inform the Member State(s) where the incident may have a significant impact. In doing so, the competent authority or the single point of contact will preserve the operator's security and commercial interests as well as the confidentiality of the information provided by the operator.</u>	The thrust of the AM for a new par.2a was included in the Council text but no conclusion as yet

¹⁴ The Council requires further consideration of this provision, including the question whether the substance of the provision should be moved to a recital or whether the provision should be supplemented by a recital explaining *inter alia* the meaning of "significant impact".

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	<u>AM103</u> <i>2b. Where the notification contains personal data, it shall be only disclosed to recipients within the notified competent authority or single point of contact who need to process those data for the performance of their tasks in accordance with data protection rules. The disclosed data shall be limited to what is necessary for the performance of their tasks.</i>		Not yet discussed in Council
	<u>AM104</u> <i>2c. Market operators not covered by Annex II may report incidents as specified in Article 14(2) on a voluntary basis.</i>		Not yet discussed in Council
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 <u>to and 2b</u> apply to all market operators providing services within the European Union.	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<p>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.</p>	<p><u>AM 105</u> 4. <i>After consultation with the notified competent authority and the market operator concerned, the single point of contact may inform the public about individual incidents, where it determines that public awareness is necessary to prevent an incident or deal with an ongoing incident, or where that market operator, subject to an incident, has refused to address a serious structural vulnerability related to that incident without undue delay.</i></p>	<p>4. <u>After consultation between the competent authority and the market operator concerned, the single point of contact competent authority</u> may inform the public, or require the market operators and public administrations to do so, <u>about individual incidents, where public awareness is necessary to prevent it</u> determines that disclosure of the an incident or deal with an ongoing incident is in the public interest. Once a year, the <u>single point of contact competent authority</u> shall submit an <u>anonymised</u> summary report to the cooperation group network on the notifications received and the action taken in accordance with this paragraph.</p>	<p>Some text of the 1st par. of the AM has been taken over in the Council text</p>
	<p><i>Before any public disclosure, the notified competent authority shall ensure that the market operator concerned has the possibility to be heard and that the decision for public disclosure is duly balanced with the public interest.</i></p>		
	<p><i>Where information about individual incidents is made public, the notified competent authority or the single point of contact shall ensure that it is made as anonymous as possible.</i></p>		

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	<i>The competent authority or the single point of contact shall, if reasonably possible, provide the market operator concerned with information that supports the effective handling of the notified incident.</i>		
	Once a year, the <i>single point of contact</i> shall submit a summary report to the cooperation network on the notifications received, <i>including the number of notifications and regarding the incident parameters as listed in paragraph 2 of this Article</i> , and the action taken in accordance with this paragraph.		
	<u>AM106</u> <i>4a. Member States shall encourage market operators to make public incidents involving their business in their financial reports on a voluntary basis.</i>		Not yet discussed in Council
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.	<u>AM107</u> <i>deleted</i>	deleted	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<p>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.</p>	<p><u>AM108</u> 6. <i>The competent authorities or the single points of contact</i> may adopt guidelines concerning the circumstances in which market operators are required to notify incidents.</p>	<p>[6. Subject to any delegated act adopted under paragraph 5, the competent authorities, <u>when requested with the assistance of ENISA,</u> may adopt guidelines and, where necessary, <u>issue instructions</u> concerning the circumstances in which market operators and public administrations are required to notify incidents.]</p>	<p>Possibly acceptable but still under consideration in the Council</p>
<p>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).</p>		<p>deleted</p>	
<p>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 enterprises¹⁵.</p>	<p><u>AM109</u> 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 enterprises³⁵, <i>unless the microenterprise acts as subsidiary for a market operator as defined in point (b) of Article 3(8).</i></p> <p>³⁵ OJ L 124, 20.5.2003, p. 36.</p>	<p>deleted</p>	<p>To be discussed further in conjunction with definition 3(8) of operator</p>

¹⁵ OJ L 124, 20.5.2003, p. 36.

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	<u>AM110</u> <i>8a. Member States may decide to apply this Article and Article 15 to public administrations mutatis mutandis.</i>		Possibly not acceptable.
<i>Article 15</i>	<i>Article 15</i>	<i>Article 15</i>	
Implementation and enforcement	Implementation and enforcement	Implementation and enforcement	
1. Member States shall ensure that the competent authorities have all the powers necessary to investigate cases of non-compliance of public administrations or market operators with their obligations under Article 14 and the effects thereof on the security of networks and information systems.	<u>AM111</u> 1. Member States shall ensure that the competent authorities and the single points of contact have the powers necessary to ensure compliance of 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 have all the powers necessary <u>means to assess investigate the cases of non-compliance of public administrations or market operators</u> and with their obligations under Article 14 and the effects thereof on the security of networks and information systems.	Possibly not acceptable
2. Member States shall ensure that the competent authorities have the power to require market operators and public administrations to:	<u>AM112</u> 2. Member States shall ensure that the competent authorities and the single points of contact have the power to require market operators to:	2. Member States shall ensure that the competent authorities <u>or the single points of contact</u> have the <u>means</u> power to require market operators and public administrations to:	Possibly not acceptable
(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;	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<p>(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.</p>	<p><u>AM113</u> (b) <i>provide evidence of effective implementation of security policies, such as the results of</i> a security audit carried out by a qualified independent body or national authority, and make the <i>evidence</i> available to the competent authority <i>or to the single point of contact</i>.</p>	<p>(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.]</p>	<p>Still under discussion in the Council</p>
	<p><u>AM114</u> NEW subparagraph 1 a <i>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.</i></p>		<p>Not clear what is meant here. What "request"?</p>
<p>3. Member States shall ensure that competent authorities have the power to issue binding instructions to market operators and public administrations.</p>	<p><u>AM115</u> 3. Member States shall ensure that <i>the</i> competent authorities <i>and the single points of contact</i> have the power to issue binding instructions to market operators.</p>	<p>3. Member States shall ensure that <u>Following the assessment of information or results of security audits referred to in paragraph 2, the competent authorities have the power to</u> may issue binding instructions to the market operators and public administrations <u>to remedy their operations.</u></p>	<p>Possibly not acceptable .</p>

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	<p><u>AM116</u> <i>3a. By way of derogation from point (b) of paragraph 2 of this Article, Member States may decide that the competent authorities or the single points of contact, as applicable, are to apply a different procedure to particular market operators, based on their level of criticality determined in accordance with Article 13a. In the event that Member States so decide:</i></p>		Possibly acceptable if less detailed
	<p><i>(a) competent authorities or the single points of contact, as applicable, shall have the power to submit a sufficiently specific request to market operators requiring them to provide evidence of effective implementation of security policies, such as the results of a security audit carried out by a qualified internal auditor, and make the evidence available to the competent authority or to the single point of contact;</i></p>		
	<p><i>(b) where necessary, following the submission by the market operator of the request referred to in point (a), the competent authority or the single point of contact may require additional evidence or an additional audit to be carried out by a qualified independent body or national authority.</i></p>		

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	<i>3b. Member States may decide to reduce the number and intensity of audits for a concerned market operator, where its security audit has indicated compliance with Chapter IV in a consistent manner.</i>		
4. The competent authorities shall notify incidents of a suspected serious criminal nature to law enforcement authorities.	<u>AM117</u> 4. The competent authorities <i>and the single points of contact shall inform the market operators concerned about the possibility of reporting incidents of a suspected serious criminal nature to the</i> law enforcement authorities.	deleted	Possibly not acceptable
5. The competent authorities shall work in close cooperation with personal data protection authorities when addressing incidents resulting in personal data breaches.	<u>AM118</u> 5. <i>Without prejudice to applicable data protection rules the 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 other Union law on data protection.</i>	5. [The competent authorities shall work in close cooperation with personal data protection authorities when addressing incidents resulting in personal data breaches.]	Possibly not acceptable. Still under consideration in the Council

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
6. Member States shall ensure that any obligations imposed on public administrations and market operators under this Chapter may be subject to judicial review.	<u>AM119</u> 6. Member States shall ensure that any obligations imposed on market operators under this Chapter may be subject to judicial review.	6. [Member States shall ensure that any obligations imposed on market operators and public administrations under this Chapter may be subject to judicial review.]	Possibly not acceptable.
	<u>AM120</u> <i>6a. Member States may decide to apply Article 14 and this Article to public administrations mutatis mutandis.</i>		Same as AM 110
<i>Article 16</i>	<i>Article 16</i>	<i>Article 16</i>	
Standardisation	Standardisation	Standardisation	
1. To ensure convergent implementation of Article 14(1), Member States shall encourage the use of standards and/or specifications relevant to networks and information security.	<u>AM121</u> 1. To ensure convergent implementation of Article 14(1), Member States, <i>without prescribing the use of any particular technology</i> , shall encourage the use <i>of European or international interoperable</i> standards and/or specifications relevant to networks and information security.	1. To promote ensure convergent implementation of Article 14(1) and 14(1a) Member States shall, <u>without prejudice to technological neutrality</u> , encourage the use of <u>European or internationally accepted</u> standards and/or specifications relevant to networks and information security.	For a large part possibly acceptable
		[1a. <u>The European Network and Information Security Agency ("ENISA"), in collaboration with Member States, may elaborate recommendations and guidelines regarding the technical areas which should be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standards, which would allow for covering these areas.</u>]	Still under consideration in the Council

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<p>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.</p>	<p><u>AM122</u> 2. The Commission shall <i>give a mandate to a relevant European standardisation body to, in consultation with relevant stakeholders</i>, draw up a list of the standards <i>and/or specifications</i> referred to in paragraph 1. The list shall be published in the Official Journal of the European Union.</p>	<p>deleted</p>	
CHAPTER V	CHAPTER V	CHAPTER V	
FINAL PROVISIONS	FINAL PROVISIONS	FINAL PROVISIONS	
<i>Article 17</i>	<i>Article 17</i>	<i>Article 17</i>	
Sanctions	Sanctions	Sanctions	
<p>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.</p>		<p>1. Member States shall lay down rules on sanctions applicable to infringements of the national provisions adopted pursuant to <u>Article 14</u> of 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.]</p>	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	<u>AM123</u> <i>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.</i>		Not yet discussed in the Council
2. Member states shall ensure that when a security incident involves personal data, the sanctions foreseen are consistent with the sanctions provided by the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data ¹⁶ .		[2. Member states shall ensure that when a security incident involves personal data, the sanctions foreseen are consistent with the sanctions provided by the [Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.]]	
<i>Article 18</i>	<i>Article 18</i>	<i>Article 18</i>	The Council deleted this article
Exercise of the delegation	Exercise of the delegation	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.		deleted	

¹⁶ SEC(2012) 72 final

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<p>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.</p>		deleted	
<p>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 <i>Official Journal of the European Union</i> or at a later date specified therein. It shall not affect the validity of any delegated act already in force.</p>	<p><u>AM124</u> 3. The delegation of power referred to in Article 9(2) 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 <i>Official Journal of the European Union</i> or at a later date specified therein. It shall not affect the validity of any delegated act already in force.</p>	deleted	
<p>4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.</p>		deleted	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<p>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.</p>	<p><u>AM125</u> 5. A delegated act adopted pursuant to Article 9(2) 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.</p>	<p>deleted</p>	
Article 19		Article 19	
Committee procedure		Committee procedure	
<p>1. The Commission shall be assisted by a committee (the Network and Information Security Committee). That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.</p>		<p>1. The Commission shall be assisted by a committee (the Network and Information Security Committee). That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.</p>	
<p>2. Where reference is made to this paragraph, Article 4 of Regulation (EU) No 182/2011 shall apply.</p>		<p>deleted</p>	
<p>3. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.</p>		<p>32. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.</p>	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
<i>Article 20</i>	<i>Article 20</i>	<i>Article 20</i>	
Review	Review	Review	
<p>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.</p>	<p><u>AM126</u> The Commission shall periodically review the functioning of this Directive, <i>in particular the list contained in Annex II</i>, and report to the European Parliament and the Council. The first report shall be submitted no later than <i>three</i> 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.</p>	<p>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(2). <u>Thereafter, the Commission shall review the functioning of this Directive every [3] years. For this purpose and with a view to further advance the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. The Commission may also request Member States to provide information without undue delay.</u></p>	<p>AM not yet discussed in Council ("the list in Annex II"), as this list can be subject to change</p>
<i>Article 21</i>	<i>Article 21</i>	<i>Article 21</i>	
Transposition	Transposition	Transposition	
<p>4. Member States shall adopt and publish, by [one year and a half after adoption] at the latest, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith communicate to the Commission the text of such provisions.</p>		<p>[1. Member States shall adopt and publish, by [two years one year and a half after adoption. <u>after the date of entry into force of this Directive</u>] at the latest, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith communicate to the Commission the text of such provisions.]</p>	<p>Still under consideration in the Council, also in regard of the timing of the establishment of the Coop. Gr. and the CSIRTs network</p>

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
They shall apply those measures from [one year and a half after adoption].		2. They shall apply those measures from [two years one year and a half after adoption the <u>date of entry into force</u> of this Directive].	
When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.		When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.	
5. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.		3. Member States <u>may</u> shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.	
<i>Article 22</i>	<i>Article 22</i>	<i>Article 22</i>	
Entry into force	Entry into force	Entry into force	
This Directive shall enter into force on the [twentieth] day following that of its publication in the <i>Official Journal of the European Union</i> .		This Directive shall enter into force on the [twentieth] day following that of its publication in the <i>Official Journal of the European Union</i> .	
<i>Article 23</i>	<i>Article 23</i>	<i>Article 23</i>	
Addressees	Addressees	Addressees	
This Directive is addressed to the Member States.		This Directive is addressed to the Member States.	
Done at Brussels,		Done at Brussels,	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
ANNEX I	ANNEX I	ANNEX I	Annex I and the EP AMs are still under consideration in the Council
Requirements and tasks of the Computer Emergency Response Team (CERT)	AM127 Requirements and tasks of the Computer Emergency Response <i>Teams (CERTs)</i>	<u>Requirements and tasks of the Computer Security Incident Emergency Response Team (CSIRT)</u>	Possibly acceptable. OK but CERTs should be "CSIRTS"
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 CSIRT CERT shall be adequately and clearly defined and supported by national policy and/or regulation. They shall include the following elements:	
(1) Requirements for the CERT		(1) Requirements for the CSIRT CERT	
(a) The CERT shall ensure high availability of its communications services by avoiding single points of failure and have several means for being contacted and for contacting others. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.	<u>AM128</u> (a) The <i>CERTs</i> 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 <i>at all times</i> . Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.	(a) The CSIRT 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.	24/7 availability still to be discussed in Council
(b) The CERT shall implement and manage security measures to ensure the confidentiality, integrity, availability and authenticity of information it receives and treats.		(b) The CSIRT CERT shall implement and manage security measures to ensure the confidentiality, integrity, availability and authenticity of information it receives and treats.	
(c) The offices of the CERT and the supporting information systems shall be located in secure sites.	<u>AM129</u> (c) The offices of the <i>CERTs</i> and the supporting information systems shall be located in secure sites <i>with secured network information systems</i> .	(c) The offices of the CSIRT CERT and the supporting information systems shall be located in secure sites.	Not yet discussed in Council

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
(d) A service management quality system shall be created to follow-up on the performance of the CERT and ensure a steady process of improvement. It shall be based on clearly defined metrics that include formal service levels and key performance indicators.		(d) A service management quality system shall be created to follow-up on the performance of the <u>CSIRT CERT</u> and ensure a steady process of improvement. It shall be based on clearly defined metrics that include formal service levels and key performance indicators.	
(e) Business continuity:		(e) Business continuity:	
– The CERT shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers,		- The <u>CSIRT CERT</u> shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers,	
– The CERT shall be adequately staffed to ensure availability at all times,		- The <u>CSIRT CERT</u> shall be adequately staffed to ensure availability at all times,	
– The CERT shall rely on an infrastructure whose continuity is ensured. To this end, redundant systems and backup working space shall be set up for the CERT to ensure permanent access to the means of communication.		- The <u>CSIRT CERT</u> shall rely on an infrastructure whose continuity is ensured. To this end, redundant systems and backup working space shall be set up for the <u>CSIRT CERT</u> to ensure permanent access to the means of communication.	
(2) Tasks of the CERT		(2) Tasks of the <u>CSIRT CERT</u>	
(a) Tasks of the CERT shall include at least the following:		(a) Tasks of the <u>CSIRT CERT</u> shall include at least the following:	
– Monitoring incidents at a national level,	<u>AM130</u> – Detecting and monitoring incidents at a national level,	- Monitoring incidents at a national level,	"Detecting" incidents in addition to "monitoring" could possibly be considered
– Providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents,		- Providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents,	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
– Responding to incidents,		- Responding to incidents,	
– Providing dynamic risk and incident analysis and situational awareness,		- Providing dynamic risk and incident analysis and situational awareness,	
– Building broad public awareness of the risks associated with online activities,		[- Building broad public awareness of the risks associated with online activities,]	
	<u>AM131</u> <i>- Actively participating in Union and international CERT cooperation networks</i>		"CERT participation in cooperation networks" could possibly be considered
– Organising campaigns on NIS;		[- Organising campaigns on NIS;]	
(b) The CERT shall establish cooperative relationships with private sector.		(b) The CSIRT CERT shall establish cooperative relationships with private sector.	
(c) To facilitate cooperation, the CERT shall promote the adoption and use of common or standardised practises for:		(c) To facilitate cooperation, the CSIRT CERT shall promote the adoption and use of common or standardised practises for:	
– incident and risk handling procedures,		- incident and risk handling procedures,	
– incident, risk and information classification schemes,		- incident, risk and information classification schemes,	
– taxonomies for metrics,		- taxonomies for metrics,	
– information exchange formats on risks, incidents, and system naming conventions.		- information exchange formats on risks, incidents, and system naming conventions.	

COMMISSION ANNEX II	EUROPEAN PARLIAMENT ANNEX II	COUNCIL ANNEX II ¹⁷	COMMENTS ON EP AMs
			Annex II and the EP AMs are still under consideration in the Council
List of market operators	List of market operators	<u>List of market operators types of entities for the purposes of Article 3(8)</u>	
Referred to in Article 3(8) a):	<u>AM132</u> <i>deleted</i>	Referred to in Article 3(8) a): <u>0. In the field of digital Internet infrastructure:</u>	
		<u>Internet exchange points¹⁸</u>	
		<u>national domain name registries, domain name system service providers</u>	
Referred to in Article (3(8) b):	<u>AM132 (con'd)</u> <i>deleted</i>	<u>0.1 In the field of service platforms:</u>	

¹⁷ In the understanding of the Council and as far as the list of (sub)sectors in Annex II is concerned, the purpose here is to achieve minimum harmonisation: Member States may add additional (sub)sectors (i.e. types of entities) to the list (and even add additional fields). Furthermore, a Member State, following the assessment on the basis of Article 3(8), may decide that, on its territory, not all entities listed in Annex II fulfil those criteria and therefore there is no risk for this or that (sub)sector. It should be noted further that it is largely immaterial whether the content of Annex II is located in an Annex or as part of art. 3, as long as the Annex may only be amended through the full legislative procedure.

¹⁸ To the extent that they are not covered by the Framework Directive.

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
1. e-commerce platforms	<u>AM132 (con'd)</u> <i>deleted</i>	1. e-commerce platforms	
2. Internet payment gateways		[2. Internet payment gateways]	
3. Social networks		[3. Social networks]	
4. Search engines		4. Search engines	
5. Cloud computing services		5. Cloud computing services, <u>including web hosting services</u> ¹⁹	
6. Application stores		[6. Application stores]	

¹⁹ The following text for a new Recital has been suggested: "Cloud computing services may comprise "infrastructure as a service" (i.e. enterprise infrastructure such as private clouds and virtual local area networks, in which a business can store its data and run the applications needed for its daily operation; and "cloud hosting", the hosting of websites on virtual servers which are founded upon pooled resources from underlying physical servers) or "platform as a service" (i.e. online computing platforms which typically include operating system, programming language execution environment, database and web server). Except where already provided for in contractual obligations between the relevant parties, a cloud computing service should be considered to fall within scope of the requirements of this Directive when it is used by an operator in the provision of an essential service. A cloud computing service provided directly to an end user other than a market operator as defined in Article 3(8) may also fall within scope of the requirements of this Directive to the extent that a Member State identifies it as a service platform underpinning the Internet that meets the definition of market operator."

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
1. Energy ²⁰	<u>AM133</u> 1. Energy <i>(a) Electricity</i>	1. <u>In the field of energy</u>	
– Electricity and gas suppliers	- Suppliers	- Electricity and gas suppliers	
– Electricity and/or gas distribution system operators and retailers for final consumers	- Distribution system operators and retailers for final consumers	- Electricity and/or gas distribution system operators and retailers for final consumers	
– Natural gas transmission system operators, storage operators and LNG operators	<i>deleted</i>	- Natural gas transmission system operators, storage operators and LNG operators	
– Transmission system operators in electricity	- Transmission system operators in electricity	- Transmission system operators in electricity	
	<i>(b) Oil</i>		
– Oil transmission pipelines and oil storage	- Oil transmission pipelines and oil storage	- Oil transmission pipelines and oil storage	
	<i>- Operators of oil production, refining and treatment facilities, storage and transmission</i>		
	<i>(c) Gas</i>		

²⁰ Cion justification for the inclusion of this field: Generation, transmission and distribution of energy are highly dependent on secure network and information systems. Ensuring the resilience of utilities is particularly important since virtually all other sectors and the well-being of our society depend upon them. For example, many major gas companies suffer increased amounts of cyber-attacks motivated by commercial and criminal intent. These attacks are posing a great risk to machinery, which can cost lives, stop production and cause environmental damage. Recent data on the number of electricity and gas companies in the EU can be found at: http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Electricity_market_indicators
http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Natural_gas_market_indicators
Furthermore, the DG ENERGY 'Report on progress in creating the Internal Gas and Electricity Market' (2009-2010) also gives some indications of the number of Transmission System Operators (TSOs) and Distribution System Operators (DSOs):
http://ec.europa.eu/energy/gas_electricity/legislation/doc/20100609_internal_market_report_2009_2010_annex.pdf
The number of electricity and gas generation, transmission and distribution operators across the EU, estimated on the basis of those sources, is approximately 4000 (**Page 70 of the Impact Assessment** provides a breakdown by countries).

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
- Electricity and gas market operators	- <i>Suppliers</i>	- Electricity and gas market operators	
	- <i>Distribution system operators and retailers for final consumers</i>		
	- <i>Natural gas transmission system operators, storage system operators and LNG system operators</i>		
- Operators of oil and natural gas production, refining and treatment facilities	- Operators of natural gas production, refining, treatment facilities, <i>storage facilities and transmission</i>	- Operators of oil and natural gas production, refining and treatment facilities	
	- <i>Gas market operators</i>		
2. Transport ²¹	<u>AM134</u> 2. Transport	2. <u>In the field of transport:</u>	

²¹ Cion justification for the inclusion of this field: The considerations done for energy are overall valid for the transport sector where a NIS incident is very likely to have "network effects" with an impact for other players in the same sector as well as for customers. This holds true for air, maritime transport and railways and for key transport infrastructure, such as airports, ports, railways, and traffic management systems and logistics. For example, aviation infrastructure (including ground and in-flight Air Traffic Management) relies on continuous and uninterrupted information flows and databases, which cannot be allowed to fail. Airports and border gateways are dependent on information assurance regarding data, control systems, networks and protocols that support the effective functioning of aviation. Both the energy and the transport sector heavily rely on Industrial Control Systems (ICS), i.e. complex computer and information systems that can be located either in one site (e.g. power plants) or distributed over a geographical area (energy and transport networks). There are numerous interconnection points between ICS, including over the Internet, and securing them is of the essence. Also, many ICS were designed in the past without anticipating the security threats posed by technological advancements. For example, remote controlling of ICS is often done via simple laptops or other mobile devices which may have a lower level of security than the rest of the system. The total number of companies across the EU that would be impacted by being in the scope is estimated to be approximately 14600 (**Page 74 of the Impact assessment** provides a background per sector and countries) based mainly on Eurostat data. For example, the number of railway operators in the EU can be found in Eurostat (total of infrastructure managers, integrated companies and railway transport operators. For maritime, Eurostat provides information on the number of sea and coastal passenger water transport companies and the number of sea and coastal freight water transport companies per Member State. As for the infrastructure, i.e. the ports, the European Commission (DG MOVE) states there are about 1 200 ports in the EU, and by lack of readily available data per Member State, this total is distributed over the individual Member States according to the distribution of freight maritime transport companies (this does not influence results for the EU total, but has as a consequence that the data at Member State level should be treated with caution). For auxiliary logistics services, the EU statistical system includes 'warehousing and support activities for transportation', of which a) warehousing and storage, b) cargo handling¹²⁴ and c) other transportation support activities are the most relevant.

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
- Air carriers (freight and passenger air transport)		- Air carriers (freight and passenger air transport)	
- Maritime carriers (sea and coastal passenger water transport companies and sea and coastal freight water transport companies)		- Maritime carriers (sea and coastal passenger water transport companies and sea and coastal freight water transport companies)	
- Railways (infrastructure managers, integrated companies and railway transport operators)		- Railways (infrastructure managers, integrated companies and railway transport operators)	
- Airports		- Airports	
- Ports		- Ports	
- Traffic management control operators		- Traffic management control operators	
- Auxiliary logistics services (a) warehousing and storage, b) cargo handling and c) other transportation support activities)		[- Auxiliary logistics services (a) warehousing and storage, b) cargo handling and c) other transportation support activities)]	
	<i>(a) Road transport</i>		
	<i>(i) Traffic management control operators</i>		
	<i>(ii) Auxiliary logistics services:</i>		
	<i>- warehousing and storage,</i>		
	<i>- cargo handling, and</i>		
	<i>- other transportation support activities</i>		
	<i>(b) Rail transport</i>		

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	<i>(i) Railways (infrastructure managers, integrated companies and railway transport operators)</i>		
	<i>(ii) Traffic management control operators</i>		
	<i>(iii) Auxiliary logistics services:</i>		
	<i>- warehousing and storage,</i>		
	<i>- cargo handling, and</i>		
	<i>- other transportation support activities</i>		
	<i>(c) Air transport</i>		
	<i>(i) Air carriers (freight and passenger air transport)</i>		
	<i>(ii) Airports</i>		
	<i>(iii) Traffic management control operators</i>		
	<i>(iv) Auxiliary logistics services:</i>		
	<i>- warehousing,</i>		
	<i>- cargo handling, and</i>		
	<i>- other transportation support activities</i>		
	<i>(d) Maritime transport</i>		
	<i>(i) Maritime carriers (inland, sea and coastal passenger water transport companies and inland, sea and coastal freight water transport companies)</i>		

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
3. Banking: credit institutions in accordance with Article 4.1 of Directive 2006/48/CE. ²²		3. <u>In the field of banking</u> : credit institutions in accordance with Article 4.1 of Directive 2006/48/CE.	
4. Financial market infrastructures: stock exchanges ²³ and central counterparty clearing houses	AM135 4. Financial market infrastructures: <i>regulated markets, multilateral trading facilities, organised trading facilities</i> and central counterparty clearing houses	4. <u>In the field of financial market infrastructures</u> : stock exchanges and central counterparty clearing houses	

²² Cion justification for the inclusion of this field: Banking activities should be secured since banks are the backbone of our financial system and because they are common targets of fraudsters. Indeed there are signs that attacks are increasing in this sector. McAfee reported that fraudsters, using malware, and replicating the same scheme in several countries, have attempted to steal up to € billion from accounts in Europe, the United States and Columbia. Consumers and businesses using online banking have increasingly experienced theft, particularly through viruses infecting their computers. Especially in this sector, we observe an increasing usage of third party business applications (such as those used for mobile banking). These applications, which are often cloud-based, are not part of the network and systems of the credit institution, which has no control over their security. In terms of impact of the obligations, Eurostat indicates a total number of credit institutions of 7706 for 2007. The order of magnitude of this figure is confirmed by the European Central Bank (ECB), which indicates that there were around 8200 credit institutions in the EU at the beginning of 2011.

²³ Cion justification for the inclusion of this field: The stock exchange increasingly adopts networks and information systems. Accidental disruptions or malicious attacks affecting the stock exchange in a country or affecting particularly critical stock exchanges such as the ones in London, Paris or Milan may have very significant impact on trade both in the internal market and internationally. In 2010 the London Stock Exchange experienced a serious cyber-attack at its headquarters, which compromised its trading system. In terms of impact of these obligations, the Impact Assessment analysed With the remarks above in mind, different lists of stock exchanges in the EU were analysed different data sets and concluded that the relevant number of affected actors in the EU is expected to be in the ranges of 25 to 30. Turnover and other financial information on the majority of European exchanges is available in the Federation of European Securities Exchanges' (FESE) "European Exchange Report".

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
5. Health sector: health care settings (including hospitals and private clinics) and other entities involved in health care provisions ²⁴		5. <u>In the field of</u> health sector: health care settings (including hospitals and private clinics) and other entities involved in health care provision. ²⁵	
	<u>AM136</u> <i>5a. Water production and supply</i>	6. <u>In the field of water supply:</u> [<u>drinking water and possibly other types of entities to be further considered</u>].	Under consideration in Council
	<u>AM137</u> <i>5b. Food supply chain</i>		Under consideration in Council
	<u>AM138</u> <i>5c. Internet exchange points</i>		Under consideration in Council

²⁴ Cion justification for the inclusion of this field: Hospitals and clinics are becoming the more and more reliant on sophisticated ICT systems which need to be secure to ensure continuity of service and avoid fatal disruptions. The proliferation of electronic medical devices presents unique challenges in ensuring that only known, authorized devices are able to connect to the network. Also, personal health and financial information is often target of cybercrime, particularly as the healthcare industry continues its conversion process to full patient electronic medical records. Networks, mobile devices, workstations, servers and medical devices are particularly critical in this regard and securing them is of the essence. In terms of the impact of these obligations, readily available data on the number of hospitals (and other health care players) in the EU Member States are not available. However, based on the estimation that on average there are 3 hospitals per 100 000 inhabitants (See the European Hospital and Healthcare Federation, http://www.hope.be/03activities/quality_euhospitals/eu_country_profiles/00-hospitals_in_europe-synthesis.pdf), it is estimated that a total number of 15000 hospitals would be impacted across the EU.

²⁵ It has been suggested to amend this indent with the following: "Healthcare settings and other entities involved in healthcare provision, which handle a significant amount of vital patient information".