Council of the European Union

Brussels, 3 October 2014

13848/14

Interinstitutional File: 2013/0027 (COD)

LIMITE

TELECOM 170
DATAPROTECT 130
CYBER 48
MI 731
CSC 215
CODEC 1939

NOTE

from:	Presidency
to:	Delegations
No. prev. doc.:	13143/14 TELECOM 162 DATAPROTECT 119 CYBER 44 MI 650 CSC 206 CODEC 1800
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 1st informal exploratory trilogue*

1. On12 February 2013, the Commission submitted the above mentioned proposal with Article 114 TFEU as a legal basis.[1] Following an orientation debate on the basis of a progress report at the June 2013 TTE Council[2], two further progress reports were submitted to the TTE Councils of December 2013 and June 2014.[3] It is recalled that the Impact Assessment accompanying the proposal was duly considered at the initial stage of its examination, as reported in doc. 10076/13.

[1] Doc. 6342/13.
[2] Doc. 10076 and doc. 10457/13.
[3] Doc. 16630/13 and 10097/14 respectively.

2. Under the Italian Presidency and at each meeting of the Working Party on Telecommunications and Information Society (WP TELE) during the months of July and September, a thorough examination of the detailed provisions of the proposal took place, resulting in various Presidency texts.[4] While acknowledging that no full consensus has yet emerged on the Council's stance on the proposal, the Presidency believes that the main principles and general orientations the Member States have been expressing in the process, have converged to such an extent, that it would be opportune to start exploratory talks with the European Parliament.

3. On the basis of the examination of the proposal, there are in particular three issues, where delegations have expressed the following main principles and general orientations: scope, cooperation and incident notification.

   – On scope, views appear to be merging that operators --be they private or public-- providing essential services in specific sectors (Article 3(8)) should be subject to the operative provisions of the Directive (in particular Article 14). While agreeing on making concrete improvements to network and information security (NIS) overall, key orientations expressed by Member States in this regard are: keeping the administrative burden for administrations in connection with implementation of the process to a minimum and avoiding that the security and notification requirements would put a disproportionate burden on businesses, especially start-ups.

[4] Doc. 12062/14 and doc. 13143/14.

An outstanding issue with regard to the scope is the identification of specific sectors (Annex II), where Member States should impose security and notification obligations on operators; for example, further discussions are needed on whether or not to include in Annex II information society services, banking and financial market infrastructures. As regards the sectors listed in Annex II, it should be recalled that the purpose of the Directive is to achieve minimum harmonisation; this does not prevent Member States, however, to add additional (sub)sectors to the list (and even to add additional fields). Furthermore, if a Member State finds that, following the assessment on the basis of the criteria mentioned in Article 3(8), on its territory, not all entities listed in Annex II fulfil those criteria, it may decide that there is therefore no risk for this or that (sub)sector. The Presidency acknowledges that the matter of scope needs further consideration and refinement, also considering that similar reflections are taking place in the EP, but that this does not put into question the operative provisions of the text.

– On security requirements and incident notification, delegations appear to agree that operators should take further steps to manage and minimise NIS risks and incidents and thus ensure the continuity of essential services (Article 14(1) and 14(1a)). However, further consideration is needed as regards the exact modalities, according to which incidents should be notified, both nationally by operators to competent authorities (Article 14(2) and (2a)) as well as in the EU context in terms of relevant national authorities notifying their EU counterparts (Article 14(2b)). Although all Member States agree that an incident notification scheme can only be effective if built on confidence and trust between all relevant actors, some delegations point to the fruitful experience gained on the basis of voluntary notification and argue that trust cannot be imposed whereas others, on the other hand, believe that the Directive should result in firm commitments as well as allow for the building of confidence and trust over time. As this is seems to be a matter of principle, exploratory talks with the EP could help in finding the right balance in the text.

– On the issue of what kind of cooperation would be needed in the context of improving NIS in the EU, there seems to be a general agreement that there is a need for a cooperation group at EU level (Article 8a), which addresses NIS matters at a strategic level (Article 8a(3)) and which guides the activities undertaken at an operational level (Article 8a(3)a). At an operational level, a CSIRTs network shall be set up, where national CSIRTs (Computer Emergency Incident Response Teams) come and work together in the area of NIS, thereby contributing to developing confidence and trust between the Member States (Article 8b). Although the tasks of the CSIRTs network include, *inter alia*, providing mutual assistance and identifying a coordinated response in case of incidents on a voluntary basis (Article 8b3(d) & (e)), some Member States wish a stronger, longer-term commitment in this regard, e.g. by tasking the CSIRTs network to produce guidelines on advanced forms of operational cooperation; other delegations, however, believe that further operational cooperation should be assessed once the necessary level of confidence and trust has been created. In any case, as the text of the proposal currently stands, both the cooperation group (Article 8a(4)) as well as the CSIRTs network (Article 8b(4)) shall provide input to the Commission's period review of the Directive (Article 20) with a view to further advance the strategic and operational cooperation.

4. At a first exploratory trilogue with the EP, which is planned to take place on 14 October, the Parliament is expected to clarify its stance following the adoption in first reading on 13 March 2014 of a legislative resolution and of 138 amendments.[5] The initial rapporteur for this file, Mr. Schwab, has been re-elected and has recently been mandated to start talks with the Council. For its part, the Presidency will inform the EP where the Council stands with its examination of the proposal, explain that the text inserted in the 3rd column of the attached 4-column document reflects the main views of the delegations expressed so far (and which should not be interpreted as the Council's final position) and give a first indication (in the 4th column) of the Council's impression of EP's first reading amendments.

[5] Doc. 7451/14.

5. Most importantly, the Presidency will present the main principles and general orientations the Member States have been expressing in the examination process, as described in point 3 above, and which shall guide the Presidency's stance in the talks with the EP. The exploratory trilogue is expected to result in the identification of issues, which require a political solution at further trilogues, and of outstanding technical matters, possible solutions for which could be drafted in technical meetings. The Presidency plans to debrief the Coreper on the outcome of the trilogue on 17 October while the WP TELE will be fully involved in the preparations for the contacts with the EP and in the examination of possible draft compromise solutions.

6. Taking the above mentioned into account, the Presidency invites the Coreper to grant it a general mandate to start exploratory talks with the Parliament on the basis of the main principles and general orientations set out above.

Proposal for a
Directive of the European Parliament and of the Council
concerning measures to facilitate ~~ensure~~ a high common level of network and information security across the Union [6]

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
CHAPTER I		**CHAPTER I**	
GENERAL PROVISIONS		**GENERAL PROVISIONS**	
Article 1		***Article 1***	
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 facilitate ~~ensure~~ a high common level of network and information security (hereinafter referred to as "NIS") within the Union so as to improve the functioning of the internal market.	
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 serious risks and incidents affecting networks and information systems;	

[6] 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
(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;	AM40 (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 ***and effective*** handling of and response to risks and incidents affecting network and information systems ***with the participation of relevant stakeholders***;	(b) creates a cooperation group ~~mechanism~~ between Member States in order to support and facilitate strategic cooperation and the exchange of information among Member States ~~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~~;	Participation of stakeholders in Coop. Group is covered in Art.8a
		(ba) creates a CSIRTs ("Computer Security Incident Response Team") network in order to contribute to developing confidence and trust between Member States and to promote swift, effective operational cooperation;	
(c) establishes security requirements for market operators and public administrations.	AM41 (c) establishes security requirements for market operators.	(c) establishes security and notification requirements for ~~market~~ operators ~~and public administrations~~.	"Operators" covers private and public entities referred to in Annex II, which provide essential services and fulfil specific criteria (see Article 3(8))
		(d) 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.	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
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.		3. The security and notification 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 subject to the requirements of Articles 13a and 13b of ~~that~~ Directive 2002/21/EC, nor to trust service providers 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.	
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[7]		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.[8]	

[7] OJ L 345, 23.12.2008, p. 75.
[8] OJ L 345, 23.12.2008, p. 75.

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
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[9], 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[10].	AM42 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 ***(EC) No 45/2001*** of the European Parliament and of the Council of ***18 December 2000*** on the protection of individuals with regard to the processing of personal data ***by the Community institutions and bodies*** and on the free movement of such data. ***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.***	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[11], 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].[12].	Cion/EP to propose rewording/clarification

[9] OJ L 281 , 23/11/1995 p. 31.
[10] SEC(2012) 72 final.
[11] OJ L 281 , 23/11/1995 p. 31.
[12] SEC(2012) 72 final.

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
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.		6. ~~The sharing of information within the cooperation network under Chapter III and the notifications of NIS incidents under Article 14 may require t~~The processing of personal data~~. Such processing, which is~~ necessary to meet the objectives of public interest pursued by this Directive, shall comply with the requirements laid down in ~~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.	
		[6a. 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.]	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	AM43 ***Article 1a*** ***Protection and processing of personal data***		Not yet discussed in Council. Possibly overdone.
	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.		
	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.		
	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.		
	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.		
	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.		

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
Article 2		***Article 2***	
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 facilitating ~~ensuring~~ a higher level of network and information security, without prejudice to their obligations under Union law.	
Article 3	***Article 3***	***Article 3***	
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 point (a) of Article 2 of Directive 2002/21/EC, and	
(b) any device or group of inter-connected or related devices, one or more of which, pursuant to a program, perform automatic processing of computer data, as well as	AM44 (b) any device or group of inter-connected or related devices, one or more of which, pursuant to a program, perform automatic processing of ***digital*** data, as well as	(b) any device or group of inter-connected or related devices, one or more of which, pursuant to a program, perform automatic processing of computer data, as well as	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.	AM45 (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;	AM46 (2) 'security' means the ability of a network and information system to resist, at a given level of confidence, accident or malicious action that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system; ***'security' includes appropriate technical devices, solutions and operating procedures ensuring the security requirements set out in this Directive.***	(2) "network and information security" means the ability of a network and information system to resist, at a given level of confidence, any ~~accident or malicious~~ action that compromise the availability, authenticity, integrity or ~~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
		(2a) "essential services" means economic and societal services essential for the functioning of the internal market.	
(3) "risk" means any circumstance or event having a potential adverse effect on security;	AM47 (3) 'risk' means any ***reasonably identifiable*** circumstance or event having a potential adverse effect on security;	(3) "risk" means any circumstance or event having a potential serious or actual adverse effect on network and information security;	Possibly acceptable but also possibly overdone
(4) "incident" means any circumstance or event having an actual adverse effect on security;	AM48 (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 network and information security that can lead to a substantial loss or disruption of essential services;	Possibly acceptable subject to consistency check with AM 53

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
(5) "information society service" mean service within the meaning of point (2) of Article 1 of Directive 98/34/EC;	AM49 ***deleted***	deleted	Possibly acceptable
(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 framework providing high-level vision, objectives and priorities on NIS at national level;	
(7) "incident handling" means all procedures supporting the analysis, containment and response to an incident;	AM50 (7) 'incident handling' means all procedures supporting the ***detection, prevention,*** analysis, containment and response to an incident;	(7) "incident handling" means all procedures supporting the analysis, containment and response to an incident;	Possibly 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;	AM51 ***deleted***	~~(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;~~	Possibly acceptable

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
(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.	AM52 (b) operator of infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, ***financial market infrastructures, internet exchange points, food supply chain*** and health***, 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***, a non exhaustive list of which is set out in Annex II***, insofar as the network and information systems concerned are related to its core services;***	~~(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.~~	The thrust of the AM has been taken on board in the Council definition of "operator"
		" operator" means a public or private entity referred to in Annex II, which provides an essential service in the fields of infrastructure enabling the provision of information society services, energy, transport, banking, financial markets, health and water supply and which fulfills all of the following criteria:	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
		- the service depends heavily on network and information systems;	
		- an incident to the network and information systems of the service having serious disruptive effects for critical social and economic activities, [and/]or having [serious] public safety implications.[13]	
		Each Member State shall identify on its territory entities, which meet the above definition of operator.	
	AM53 ***(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;***		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 point (1) of Article 2 of Regulation (EU) No 1025/2012;	
(10) "specification" means a specification referred to in Regulation (EU) No 1025/2012;		(10) "specification" means a technical specification referred to in point (4) of Article 2 of Regulation (EU) No 1025/2012;	

[13] The Council is considering whether additional criteria ought to be introduced here, e.g.: "an incident having a significant effect on the consumer or on other businesses heavily depending on that service", or "an incident that is local by nature but having consequences across borders." Regarding "significant effect" in the 1st suggestion, examples could be provided in a dedicated recital.

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
(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.		(11) "Trust service provider" means a natural or legal person within the meaning of point (19) of Article 3 of Regulation 910/2014 ~~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~~.	
	AM54 ***(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];*** ***----------*** ***[1a] 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).***		What is the justification for including such a definition?
	AM55 ***(11b) 'multilateral trading facility (MTF)' means multilateral trading facility as defined in point 15 of Article 4 of Directive 2004/39/EC;***		What is the justification for including such a definition?

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	AM56 ***(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;***		What is the justification for including such a definition?
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**	
Article 4		~~***Article 4***~~	
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.		~~Member States shall ensure a high level of security of the network and information systems in their territories in accordance with this Directive.~~	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
Article 5	***Article 5***	***Article 5***	
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 facilitate ~~achieve and maintain~~ a high level of network and information security at least in the fields referred to in Article 3(8). The national NIS strategy shall address in particular the following issues:	
(a) The definition of the objectives and priorities of the strategy based on an up-to-date risk and incident analysis;		(a) ~~The definition of the~~ The objectives and priorities of the national NIS strategy ~~based on an up-to-date risk and incident analysis~~;	
(b) A governance framework to achieve the strategy objectives and priorities, including a clear definition of the roles and responsibilities of the government bodies and the other relevant actors;		[(b) The ~~A~~ governance framework put in place to achieve the ~~strategy~~ objectives and priorities of the national NIS strategy, ~~including a clear definition of the roles and responsibilities of the government bodies and the other relevant actors~~;]	
(c) The identification of the general measures on preparedness, response and recovery, including cooperation mechanisms between the public and private sectors;		(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 relating to the NIS strategy;	

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.~~	
	AM57 ***(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.***		Possibly 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;	AM58 (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***;	(f) A risk assessment plan to identify potential-risks ~~and assess the impacts of potential incidents;~~	Probably too prescriptive
(b) The definition of the roles and responsibilities of the various actors involved in the implementation of the plan;	AM59 (b) The definition of the roles and responsibilities of the various ***authorities and other*** actors involved in the implementation of the ***framework***;	(g) ~~The definition of the roles and responsibilities~~ A list of the various actors involved in the implementation of the NIS strategy ~~plan~~;	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.	AM60 3. The national NIS strategy and the national NIS cooperation plan shall be communicated to the Commission within ***three months*** from their adoption.	3. The <u>Member States shall make available to the Commission at least a summary of the</u> national NIS strategy ~~and the national NIS cooperation plan shall be communicated to the Commission within one month from their adoption~~.	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	AM61 **National competent *authorities and single points of contact* on the security of network and information systems**	**National competent authorities~~y~~ and single point of contact ~~on the security of network and information systems~~**	Possibly acceptable
1. Each Member State shall designate a national competent authority on the security of network and information systems (the "competent authority").	AM62 1. Each Member State shall designate ***one or more civilian*** national competent ***authorities*** on the security of network and information systems (***hereinafter referred to as*** 'competent authority***/ies***').	1. Each Member State shall designate one or more ~~a~~ national competent authorities~~y~~ on the security of network and information systems (the "competent authority"). Member States may designate this role to an existing authority or authorities.	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	
	AM63 ***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.***	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.	EP and Council agree that MS should designate one SPC

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	AM64 ***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.***	[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.]	Possibly acceptable. in [brackets] for the time being
	AM65 ***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 the Coop. Group and with the SPCs of other MS
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.	AM66 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.	[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.]	Similar comment as for AM65

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
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.	AM67 4. Member States shall ensure that the competent authorities ***and single points of contact, where applicable in accordance with paragraph 2a of this Article,*** 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.	~~[4. Member States shall ensure that the competent authorities receive the notifications of incidents from market operators and public administrations as specified under Article 14(2)and are granted the implementation and enforcement powers referred to under Article 15.]~~	Possibly not acceptable
	AM68 ***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.***		To be assessed whether this AM doesn't make it more difficult to identify the actors implied in the process

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.	AM69 5. The competent authorities ***and single points of contact*** shall consult and cooperate, whenever appropriate, with the relevant law enforcement national authorities and data protection authorities.	[5. The competent authorities shall consult and cooperate, whenever appropriate and in accordance with national legislation, 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.	AM70 6. Each Member State shall notify to the Commission without delay the designation of the competent ***authorities and the single point of contact***, its tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent ***authorities***.	6. Each Member State shall notify to the Commission without delay the designation of the competent authorities~~y~~ and single point of contact, their ~~its~~ tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent authorities~~y~~ and single point of contact.	Reflected in Council text
Article 7	***Article 7***	***Article 7***	
Computer Emergency Response Team	**Computer Emergency Response Team**	**Computer Security Incident ~~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.	AM71 1. Each Member State shall set up ***at least one*** Computer Emergency Response Team (hereinafter: 'CERT') ***for each of the sectors established in Annex II,*** responsible for handling incidents and risks according to a well-defined process, which shall comply with the requirements set out in point (1) of Annex I. A CERT may be established within the competent authority.	1. Each Member State shall designate one or more ~~set up a~~ Computer Security Incident ~~Emergency~~ Response Teams (hereinafter: "CSIRTs ~~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 CSIRT may be established within the competent authority.	Partly taken on board.

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
		1a. Where they are separate, the competent authorities, the single point of contact and the CSIRTs ~~CERTs~~ of the same Member State shall cooperate closely with regard to the obligations laid down in this Directive.	
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.		[2. Member States shall ensure that CSIRTs ~~CERTs~~ have adequate ~~technical, financial and human~~ resources to effectively carry out their tasks set out in point (2) of Annex I.]	
3. Member States shall ensure that CERTs rely on a secure and resilient communication and information infrastructure at national level, which shall be compatible and interoperable with the secure information-sharing system referred to in Article 9.		3. Member States shall ensure that CSIRTs ~~CERTs~~ have access to an appropriate ~~rely on a secure and resilient~~ communication and information infrastructure at national level~~, which shall be compatible and interoperable with the secure information-sharing system referred to in Article 9~~.	
4. Member States shall inform the Commission about the resources and mandate as well as the incident handling process of the CERTs.		4. Member States shall inform the Commission about the remit ~~resources and mandate as well as the incident handling process~~ of the CSIRTs ~~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.	AM72 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	Possibly not acceptable

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	AM73 ***5a. Member States shall ensure that CERTs have adequate human and financial resources to actively participate in international, and in particular Union, cooperation networks***		Possibly not acceptable
	AM74 ***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.***		Not yet discussed in Council. To be cross-checked against ENISA's tasks
	AM75 ***5c. Member States may ask for the assistance of ENISA or of other Member States in developing their national CERTs.***		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 ~~CERTs~~**	
Article 8	***Article 8***	***~~Article 8~~***	
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.	AM76 1. The ***single points of contact*** and the Commission ***and ENISA*** shall form a network (***hereinafter referred to as*** 'cooperation network') to cooperate against risks and incidents affecting network and information systems.	Replaced by article 8a	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.	AM77 2. The cooperation network shall bring into permanent communication the Commission and the ***single points of contact***. When requested, ENISA shall assist the cooperation network by providing its expertise and advice. ***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.***	Replaced by article 8a	Partly covered in Council's new text for paragraph 2

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
3. Within the cooperation network the competent authorities shall:	AM78 3. Within the cooperation network the ***single points of contact*** shall:	Replaced by article 8a	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;	Replaced by article 8a	
(b) ensure a coordinated response in accordance with Article 11;	(b) ensure a coordinated response in accordance with Article 11;	Replaced by article 8a	
(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;	Replaced by article 8a	
(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***;***	Replaced by article 8a	
(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;	Replaced by article 8a	
(f) cooperate and exchange information on all relevant matters with the EuropeanCybercrime Center within Europol, and with other relevant European bodies in particular in the fields of data protection, energy, transport, banking, stock exchanges and health;	AM78 (f) cooperate and exchange ***expertise on*** relevant matters ***on network and information security,*** in particular in the fields of data protection, energy, transport, banking, ***financial markets*** and health ***with the European Cybercrime Centre within Europol, and with other relevant European bodies***;	Replaced by article 8a	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	AM78 ***(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;***		
(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;	Replaced by article 8a	
(h) organise regular peer reviews on capabilities and preparedness;		Replaced by article 8a	
(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.	Replaced by article 8a	
	AM78 ***(ia) involve, consult and exchange, where appropriate, information with market operators with respect to the risks and incidents affecting their network and information systems;***		
	AM78 ***(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.***		

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	AM79 ***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.***		To be compared with Council's newly proposed paragraph 4.
		Article 8a	
		Cooperation <u>group</u> ~~network~~	
		<u>1. In order to support and facilitate strategic cooperation and the exchange of information among Member States in the fields referred to in Article 3(8), 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. Where appropriate, representatives from the competent authorities and ~~market~~ operators shall be invited to participate in the discussions of the cooperation group.</u>	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
		3. The tasks of the cooperation group shall be to:	
		a. Provide guidance for the activities of the CSIRTs network established under Article 8b.	
		ab. Exchange best practice on the exchange of information related to incident notification referred to in Article 14(2b).[14]	
		b. Exchange best practices between Member States and, in collaboration with ENISA, assist Member States in building capacity in NIS;[15]	
		c. At the request of a Member State organise regular peer reviews on capabilities and preparedness of that same Member State;[16]	
		d. At the request of a Member State discuss the national NIS strategy of that same Member State;[17]	
		e. At the request of a Member State discuss the effectiveness of the CSIRT of that same Member State.[18]	

14 This provisions corresponds to Article 8(3)a in the Commission's proposal.
15 This provisions corresponds to Article 8(3)g in the Commission's proposal.
16 This provisions corresponds to Article 8(3)h in the Commission's proposal.
17 This provisions corresponds to Article 8(3)d in the Commission's proposal.
18 This provisions corresponds to Article 8(3)e in the Commission's proposal.

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
		f. Exchange information and best practice on awareness raising and training.	
		g. Exchange information and best practice on research and development on network and information security.	
		h. With representatives from the relevant European Standards Organisations, discuss the standards referred to in Article 16.	
		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;	
		j. In collaboration with ENISA, agree a roadmap for NIS exercises, education programmes and training.	
		k.) With ENISA´s assistance, exchange best practices with regard to the identification of operators by the Member States.	
		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.	

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

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
		2. The CSIRTs network shall be composed of representatives from the national CSIRTs, the European Network and Information Security Agency ("ENISA") and CERT-EU. The Commission shall have an observer role and provide secretariat functions.	
		3. The CSIRTs network shall have the following tasks:	
		a. Exchange high-level information on CSIRTs services, operations and cooperation capabilities.	
		b. At the request of any Member State, exchange and discuss non-commercially sensitive information related to risks and on-going incidents.	
		c. Exchange and publish anonymised information on incidents, which occurred in the past.	
		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.	
		e. Assist each other in cross-border incidents on the basis of voluntary mutual assistance.	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
		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.	
		5. The Commission shall adopt, by means of implementing acts, procedural arrangements necessary for the functioning of the network of the national CSIRTs. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(2).	
Article 9	***Article 9***	~~**Article 9**~~	
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	
	AM81 ***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.***		Council deleted art.9

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
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:	AM82 ***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	
(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	
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).	AM83 3. The Commission shall adopt, by means of ***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***.		Council deleted art.9

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
Article 10	***Article 10***	~~***Article 10***~~	Council deleted art.10
Early warnings	**Early warnings**	~~**Early warnings**~~[19]	
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:	AM84 1. The ***single points of contact*** or the Commission shall provide early warnings within the cooperation network on those risks and incidents that fulfil at least one of the following conditions:	deleted	Council deleted art.10 but included early warning in art.14. Not yet discussed in Council.
(a) they grow rapidly or may grow rapidly in scale;		deleted	
(b) they exceed or may exceed national response capacity;	(b) ***the single point of contact assesses that the risk or incident potentially exceeds*** national response capacity;	deleted	
(c) they affect or may affect more than one Member State.	(c) ***the single points of contact or the Commission assess that the risk or incident affects*** more than one Member State.	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.	AM85 2. In the early warnings, the ***single points of contact*** and the Commission shall communicate ***without undue delay*** any relevant information in their possession that may be useful for assessing the risk or incident.	deleted	Council deleted art.10 but included early warning in art.14. 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.	AM86 ***deleted***	deleted	Council deleted art.10 but included early warning in art.14. Not yet discussed in Council.

[19] 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
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.	AM87 ***deleted***	deleted	Council deleted art.10 but included early warning in art.14.
	AM88 ***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.***		Council deleted art.10 but included early warning in art.14.
	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.		
	AM89 ***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.***		Council deleted art.10 but included early warning in art.14. 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	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
Article 11	***Article 11***	~~***Article 11***~~	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.	AM90 1. Following an early warning referred to in Article 10 the ***single points of contact*** shall, after assessing the relevant information, agree ***without undue delay*** on a coordinated response in accordance with the Union NIS cooperation plan referred to in Article 12.	deleted	Possibly not acceptable.
2. The various measures adopted at national level as a result of the coordinated response shall be communicated to the cooperation network.		deleted	
Article 12	***Article 12***	~~***Article 12***~~	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	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
– 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,	AM91 – a definition of the format and procedures for the collection and sharing of compatible and comparable information on risks and incidents by the ***single points of contact***,		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	
(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.	AM92 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. ***The results of each revision shall be reported to the European Parliament.***	deleted	Possibly not acceptable

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	AM93 ***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.***		Possibly not acceptable
Article 13	***Article 13***	***Article 13***	
International cooperation	**International cooperation**	**International cooperation**	
Without prejudice to the possibility for the cooperation network to have informal international cooperation, the Union may conclude international agreements with third countries or international organisations allowing and organizing their participation in some activities of the cooperation network. Such agreement shall take into account the need to ensure adequate protection of the personal data circulating on the cooperation network.	AM94 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 ***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.***	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 group ~~network~~. Such agreement shall take into account the need to ensure adequate protection of the personal data circulating within ~~on~~ the cooperation group ~~network~~.	Not yet discussed in Council.

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	AM95 ***Article 13a*** ***Level of criticality of market operators***		The thrust of the AM is taken on board in the Council's text of Article 3(2a), 3(8).
	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.		

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**	
Article 14	***Article 14***	***Article 14***	
Security requirements and incident notification	**Security requirements and incident notification**	**Security requirements and incident notification**	
1. Member States shall ensure that public administrations and market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.	AM96 1. Member States shall ensure that market operators take appropriate ***and proportionate*** technical and organisational measures to ***detect and effectively*** manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, ***those*** measures shall ***ensure*** a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting ***the security of*** their network and information ***systems*** on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.	1. Member States shall require ~~ensure~~ that ~~market~~ operators ~~and public administrations~~ take appropriate, sector-specific technical and organisational measures to manage the risks posed to ~~the security of the~~ networks and information security of systems which they control and use in their operations. Having regard to the state of the art, these measures shall maintain ~~guarantee~~ a level of network and information security appropriate to the risk presented.	Possibly acceptable with the exception of "ensuring" security

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
		1a ~~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.	AM97 2. Member States shall ensure that market operators notify ***without undue delay*** to the competent authority ***or to the single point of contact*** incidents having a significant impact on the ***continuity*** of the core services they provide. ***Notification shall not expose the notifying party to increased liability.***	2. Member States shall provide for a reporting scheme pursuant to which ~~ensure that market~~ operators ~~and public administrations~~ shall notify without undue delay to the competent authority incidents having a significant impact on the continuity ~~security~~ of the essential ~~core~~ services they provide.	Not yet discussed in Council. Council text still under development
	To determine the significance of the impact of an incident, the following parameters shall inter alia be taken into account:	2a To determine the significance of the impact of an incident, the following parameters in particular shall be taken into account:	
	AM98 ***(a) the number of users whose core service is affected;***	a) the number of users affected by the disruption of the essential service;	Included in the Council text for the time being but still subject to further consideration
	AM99 ***(b) the duration of the incident;***	(b) the duration of the incident;	Included in the Council text for the time being but still subject to further consideration

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	AM100 ***(c) geographic spread with regard to the area affected by the incident.***	(c) the geographical spread with regard to the area affected by the incident.[20]	Included in the Council text for the time being but still subject to further consideration
	AM101 ***Those parameters shall be further specified in accordance with point (ib) of Article 8(3).***		Not yet discussed in Council. Discussion on determining the "significance" of incidents still ongoing
	AM102 ***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.***	[2b Where essential services in more than one Member State are affected, the competent authority or the single point of contact which has received the notification shall, on the basis of the information provided by the operator and after appropriate consultation with that operator, inform the single points of contact of the Member States concerned. The operator shall be informed without undue delay, which other competent authorities or 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.][21]	The thrust of the AM for a new par.2a was included in the Council text but no conclusion as yet

[20] 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".

[21] This provision is still under consideration in the Council.

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	AM103 ***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.***		Not yet discussed in Council
	AM104 ***2c. Market operators not covered by Annex II may report incidents as specified in Article 14(2) on a voluntary basis.***		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</u> ~~and~~ 2<u>b</u> apply to all ~~market~~ operators <u>established</u> ~~providing services with~~in the European Union.	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
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.	AMD 105 4. ***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.***	4. After consultation between the competent authority and the ~~market~~ operator concerned, ~~The~~ the single point of contact ~~competent authority~~ may inform the public, or require the ~~market~~ operators ~~and public administrations~~ to do so, about individual incidents, where public awareness is necessary to prevent ~~it determines that disclosure of the~~ an incident or deal with an ongoing incident ~~is in the public interest~~. Once a year, the single point of contact ~~competent authority~~ shall submit an anonymised summary report to the cooperation group ~~network~~ on the notifications received and the action taken in accordance with this paragraph.	Some text of the 1st par. of the AM has been taken over in the Council text
	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***.		
	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.		

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	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.		
	Once a year, the ***single point of contact*** shall submit a summary report to the cooperation network on the notifications received***, including the number of notifications and regarding the incident parameters as listed in paragraph 2 of this Article,*** and the action taken in accordance with this paragraph.		
	AM106 ***4a. Member States shall encourage market operators to make public incidents involving their business in their financial reports on a voluntary basis.***		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.	AM107 ***deleted***	deleted	Possibly acceptable. The Council also deleted par.5 on delegated acts.

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
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.	AM108 6. ***The competent authorities or the single points of contact*** may adopt guidelines concerning the circumstances in which market operators are required to notify incidents.	[6. ~~Subject to any delegated act adopted under paragraph 5, t~~The competent authorities, when requested with the assistance of ENISA, may adopt guidelines ~~and, where necessary, issue instructions~~ concerning the circumstances in which ~~market~~ operators ~~and public administrations~~ are required to notify incidents.]	Possibly acceptable. Taken on board
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).		deleted	
8. Paragraphs 1 and 2 shall not apply to microenterprises as defined in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises[22].	AM109 8. Paragraphs 1 and 2 shall not apply to microenterprises as defined in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises[35], ***unless the microenterprise acts as subsidiary for a market operator as defined in point (b) of Article 3(8)***. [35] OJ L 124, 20.5.2003, p. 36.	deleted	Possibly acceptable

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

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	AM110 ***8a. Member States may decide to apply this Article and Article 15 to public administrations mutatis mutandis.***		Possibly not acceptable.
Article 15	***Article 15***	***Article 15***	
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.	AM111 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 means to assess ~~investigate~~ the ~~cases of non-~~ compliance of ~~public administrations or market~~ operators ~~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:	AM112 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 or the single points of contact have the means ~~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
(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.	AM113 (b) ***provide evidence of effective implementation of security policies, such as the results of*** a security audit carried out by a qualified independent body or national authority**,** and make the ***evidence*** available to the competent authority ***or to the single point of contact***.	(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.]	Not yet discussed in Council
	AM114 NEW subparagraph 1 a ***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.***		Not clear what is meant here. What "request"?
3. Member States shall ensure that competent authorities have the power to issue binding instructions to market operators and public administrations.	AM115 3. Member States shall ensure that ***the*** competent authorities ***and the single points of contact*** have the power to issue binding instructions to market operators.	3. ~~Member States shall ensure that~~ Following the assessment of information or results of security audits referred to in paragraph 2, the competent authorities ~~have the power to~~ may issue ~~binding~~ instructions to the ~~market~~ operators ~~and public administrations~~ to remedy their operations.	Possibly not acceptable .

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	AM116 ***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:***		Possibly acceptable if less detailed
	(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;		
	(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.		

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	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.		
4. The competent authorities shall notify incidents of a suspected serious criminal nature to law enforcement authorities.	AM117 4. The competent authorities ***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*** law enforcement authorities.	deleted	poss. acceptable
5. The competent authorities shall work in close cooperation with personal data protection authorities when addressing incidents resulting in personal data breaches.	AM118 5. ***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.***	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

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.	AM119 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.
	AM120 ***6a. Member States may decide to apply Article 14 and this Article to public administrations mutatis mutandis.***		Same as AM 110
Article 16	**Article 16**	***Article 16***	
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.	AM121 1. To ensure convergent implementation of Article 14(1), Member States***, without prescribing the use of any particular technology,*** shall encourage the use ***of European or international interoperable*** 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, without prejudice to technological neutrality, encourage the use of internationally accepted standards and/or specifications relevant to networks and information security.	1st part taken on board, 2nd ("European or international interoperable") too prescriptive and self-evident
		[1a. 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.]	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
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.	AM122 2. The Commission shall ***give a mandate to a relevant European standardisation body to***, ***in consultation with relevant stakeholders,*** draw up a list of the standards ***and/or specifications*** referred to in paragraph 1. The list shall be published in the Official Journal of the European Union.	deleted	Possibly not acceptable.
CHAPTER V	**CHAPTER V**	**CHAPTER V**	
FINAL PROVISIONS	**FINAL PROVISIONS**	**FINAL PROVISIONS**	
Article 17	***Article 17***	***Article 17***	
Sanctions	**Sanctions**	**Sanctions**	
1. Member States shall lay down rules on sanctions applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The sanctions provided for must be effective, proportionate and dissuasive. The Member States shall notify those provisions to the Commission by the date of transposition of this Directive at the latest and shall notify it without delay of any subsequent amendment affecting them.		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.]	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	AM123 ***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.***		Not yet discussed in 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[23].		[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.]]	
Article 18	***Article 18***	~~***Article 18***~~	
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	

[23] SEC(2012) 72 final

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
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.		deleted	
3. The delegation of powers referred to in Articles 9(2), 10(5) and 14(5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the powers specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated act already in force.	AM124 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 Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated act already in force.	deleted	Possibly not acceptable.
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.		deleted	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
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.	AM125 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.	deleted	Possibly not acceptable.
Article 19		***Article 19***	
Committee procedure		**Committee procedure**	
1. The Commission shall be assisted by a committee (the Network and Information Security Committee). That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.		1. The Commission shall be assisted by a committee (the Network and Information Security Committee). That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.	
2. Where reference is made to this paragraph, Article 4 of Regulation (EU) No 182/2011 shall apply.		deleted	
3. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.		~~3~~**2**. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
Article 20	***Article 20***	***Article 20***	
Review	**Review**	**Review**	
The Commission shall periodically review the functioning of this Directive and report to the European Parliament and the Council. The first report shall be submitted no later than three years after the date of transposition referred to in Article 21. For this purpose, the Commission may request Member States to provide information without undue delay.	AM126 The Commission shall periodically review the functioning of this Directive***, in particular the list contained in Annex II,*** and report to the European Parliament and the Council. The first report shall be submitted no later than ***three*** years after the date of transposition referred to in Article 21. For this purpose, the Commission may request Member States to provide information without undue delay.	The Commission shall 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). 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.	Not yet discussed in Council "the list in Annex II", as this list can be subject to change (i.e. if this list is maintained)
Article 21	***Article 21***	***Article 21***	
Transposition	**Transposition**	**Transposition**	
4. Member States shall adopt and publish, by [one year and a half after adoption] at the latest, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith communicate to the Commission the text of such provisions.		1. Member States shall adopt and publish, by [two years ~~one year and a half after adoption~~. after the date of entry into force of this Directive] 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.	

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~~ date of entry into force 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 may ~~shall~~ communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.	
Article 22	***Article 22***	***Article 22***	
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 *Official Journal of the European Union.*		This Directive shall enter into force on the [twentieth] day following that of its publication in the *Official Journal of the European Union.*	
Article 23	***Article 23***	***Article 23***	
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**	
Requirements and tasks of the Computer Emergency Response Team (CERT)	AM127 Requirements and tasks of the Computer Emergency Response ***Teams (CERTs)***	**Requirements and tasks of the Computer Security Incident ~~Emergency~~ Response Team (CSIRT)**	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.	AM128 (a) The ***CERTs*** shall ensure high availability of its communications services by avoiding single points of failure and have several means for being contacted and for contacting others ***at all times***. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.	(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.	AM129 (c) The offices of the ***CERTs*** and the supporting information systems shall be located in secure sites ***with secured network information systems.***	(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 CSIRT ~~CERT~~ and ensure a steady process of improvement. It shall be based on clearly defined metrics that include formal service levels and key performance indicators.	
(e) Business continuity:		(e) Business continuity:	
– The CERT shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers,		- The CSIRT ~~CERT~~ shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers,	
– The CERT shall be adequately staffed to ensure availability at all times,		- The CSIRT ~~CERT~~ shall be adequately staffed to ensure availability at all times,	
– The CERT shall rely on an infrastructure whose continuity is ensured. To this end, redundant systems and backup working space shall be set up for the CERT to ensure permanent access to the means of communication.		- The CSIRT ~~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 CSIRT ~~CERT~~ to ensure permanent access to the means of communication.	
(2) Tasks of the CERT		(2) Tasks of the CSIRT ~~CERT~~	
(a) Tasks of the CERT shall include at least the following:		(a) Tasks of the CSIRT ~~CERT~~ shall include at least the following:	
– Monitoring incidents at a national level,	AMD 130 – ***Detecting and*** monitoring incidents at a national level,	- Monitoring incidents at a national level,	"Detecting" incidents in addition to "monitoring" could 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,**]**	
	AM131 ***- Actively participating in Union and international CERT cooperation networks***		"CERT participation in cooperation networks" could 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	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
ANNEX II	**ANNEX II**	**ANNEX II**	
List of market operators	**List of market operators**	**List of ~~market~~ ~~operators~~ types of entities for the purposes of Article 3(8)**[24]	
Referred to in Article 3(8) a):	AM132 ***deleted***	~~Referred to in Article 3(8) a):~~	
		0. In the field of infrastructure enabling the provision of information society services:	
		Internet exchange points	
		national domain name registries	
		web hosting services	
1. e-commerce platforms 2. Internet payment gateways 3. Social networks 4. Search engines 5. Cloud computing services 6. Application stores	AM132 ***deleted***	e-commerce platforms Internet payment gateways Social networks Search engines Cloud computing services Application stores	
Referred to in Article (3(8) b):		~~Referred to in Article (3(8) b):~~	
1. Energy	AM133 1. Energy ***(a) Electricity***	1. In the field of energy	Under consideration in Council
– Electricity and gas suppliers	- Suppliers	- Electricity and gas suppliers	

[24] 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.

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
– 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	***deleted***	- 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	
	(b) Oil		
– Oil transmission pipelines and oil storage	- Oil transmission pipelines and oil storage	- Oil transmission pipelines and oil storage	
	- Operators of oil production, refining and treatment facilities, storage and transmission		
	(c) Gas		
– Electricity and gas market operators	***- Suppliers***	- Electricity and gas market operators	
	- Distribution system operators and retailers for final consumers		
	- Natural gas transmission system operators, storage system operators and LNG system operators		
– Operators of oil and natural gas production, refining and treatment facilities	- Operators of natural gas production, refining, treatment facilities, ***storage*** facilities ***and transmission***	- Operators of oil and natural gas production, refining and treatment facilities	
	- Gas market operators		
2. Transport	AM134 2. Transport	2. <u>In the field of</u> transport :	Under consideration in Council
– Air carriers (freight and passenger air transport)	***(a) Road transport***	- Air carriers (freight and passenger air transport)	

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

COMMISSION	EUROPEAN PARLIAMENT	COUNCIL	COMMENTS ON EP AMs
	- warehousing,		
	- cargo handling, and		
	- other transportation support activities		
	(d) Maritime transport		
	(i) Maritime carriers (inland, sea and coastal passenger water transport companies and inland, sea and coastal freight water transport companies)		
3. Banking: credit institutions in accordance with Article 4.1 of Directive 2006/48/CE.		3. In the field of banking: credit institutions in accordance with Article 4.1 of Directive 2006/48/CE.	
4. Financial market infrastructures: stock exchanges and central counterparty clearing houses	AM135 4. Financial market infrastructures: ***regulated markets, multilateral trading facilities, organised trading facilities*** and central counterparty clearing houses	4. In the field of financial market infrastructures: stock exchanges and central counterparty clearing houses	Under consideration in Council
5. Health sector: health care settings (including hospitals and private clinics) and other entities involved in health care provisions		5. In the field of health sector: health care settings (including hospitals and private clinics) and other entities involved in health care provision.	
	AM136 ***5a. Water production and supply***		Under consideration in Council
	AM137 ***5b. Food supply chain***		Under consideration in Council
	AM138 ***5c. Internet exchange points***		Under consideration in Council
		6. In the field of water supply: [types of entities to be further considered].	