Council of the European Union

Brussels, 3 December 2015
(OR. en)

Interinstitutional File: 2013/0027 (COD)

14606/2/15 REV 2

LIMITE

TELECOM 222
DATAPROTECT 217
CYBER 111
MI 762
CSC 293
CODEC 1593

NOTE

From:	Presidency
To:	Permanent Representatives Committee
No. prev. doc.:	14352/15 TELECOM 218 DATAPROTECT 206 CYBER 109 MI 733 CSC 284 CODEC 1552
No. Cion doc.:	6342/13 TELECOM 24 DATAPROTECT 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 - Preparation for the trilogue

1. On 13 November and on the basis of doc. 13754/1/15 REV 1, the Coreper granted the Presidency a mandate to resume informal exploratory talks with the EP on the above mentioned proposal. A fifth exploratory trilogue took place on 17 November and the Presidency informed the Coreper about the results of this event on 20 November.

2. In view of the next and hopefully final informal trilogue, which is planned to take place on 7 December, the Presidency now seeks an updated mandate on the basis of a text presented in the 3rd and 4th columns of the annexed 4-column table (the 3rd column remains valid unless a compromise proposal is introduced in the 4th column). This text is the result of detailed examination in the Council's WP TELE and of numerous technical meetings with the EP. It is also in line with the main principles set out in the cover note of doc. 13754/1/15, which still stand for the upcoming informal trilogue.

3. The key outstanding issues expected to be discussed at the informal trilogue are the following:

   a) With regard to operators of essential services, the majority of the text can be considered agreed in principle, even though some slight, mainly textual, differences will still need to be ironed out, e.g. in connection with art. 14(6) on guidelines with regard to the circumstance for notification of incidents or art. 20a(1a) with regard to the role of the cooperation group in the discussion of national measures on identification. The most important issue in this area will therefore be the question of jurisdiction. The European Parliament is not convinced that the Council's text in art. 3a(1) provides for enough legal certainty and will likely request further clarifications of this provision. Another question that will need to be solved at the trilogue is the question of inclusion of auxilliary logistic services for road transport in Annex II on which the European Parliament strongly insists. Delegations are invited to indicate whether they could show some flexibility in this respect in the spirit of compromise.

   b) The main outstanding issue for the trilogue will be the question of digital service providers. The discussions at the previous trilogue already allowed to identify elements where the positions of the institutions are very close to each other, in particular with regard to the 'light touch' approach and the exclusion of micro and small enterprises. The main differences appear to be in the following areas:

- the level of harmonisation: It is clear that this issue will be one of the key points for the discussion at the trilogue. The European Parliament that originally did not want to include digital service providers in the Directive, subjects the inclusion to the condition of maximum harmonisation. It argues that this is part of the 'light touch' approach making sure that digital service providers are not subject to different requirements in different Member States. The Council's proposal for jurisdiction based on the principle of main establishment (which seems to be accepted by the European Parliament) addresses this issue only partially since it ensures that one digital service provider is only subject to requirements of the Member State where it is established, but still allows for different requirements for similar providers established in other Member States. The European Parliament has provided a proposal on how to achieve the maximum harmonisation, which, in particular, consists in providing for a delegated act on security and notification requirements for digital service providers. The Presidency would propose a compromise solution based on the following elements:

- exclusion of art. 15a(1), (1a) and (2) from article 2 on minimum harmonisation;
- some streamlining of the security requirement in article 15a(1) ; and
- complemeting of article 15a(2) on notification of substantial incidents.

- list of services to be covered in Annex III: The remaining difference in this regard is that the European Parliament does not support the inclusion of social networks in the Annex III.

- definitions: the European Parliament made it clear during the fifth trilogue that its acceptance of the inclusion of digital service providers in the Directive is subject to the condition that the definitions are sufficiently clear and precise. The Council shares this objective but the final wording is still to be discussed. With regard to the general definition of digital service provider (art. 3(8a)), the European Parliament does not accept the phrase 'offered to public at large and to businesses at large'. Therefore it will be necessary to find a suitable compromise solution for this issue. Moreover, the European Parliament insists that, for the purposes of better legislative technique, the definitions of digital services that are now included in Annex III should be included together with other definitions in art. 3. The Presidency believes that this wish could be accommodated in the context of an overall package deal while a recital can clarify that the definitions are applicable solely for the purposes of this Directive.

c) With regard to horizontal issues, the Presidency expects a debate on transposition and other deadlines, where the European Parliament insists that the overall timeline should be shorter than that envisaged in the Council text. With regard to art. 1(7) on lex specialis, while the European Parliament shares the Council's political objective that the use of that provision should not lead to lower requirements, it is of the view that clearer language should be used to avoid legal uncertainty. The Presidency has suggested to replace the word 'comparable' with 'equivalent' and provided for three clarifying recitals.

4. The Council text (doc. 14352/15) was discussed in the WP TELE meeting of 26 November and, based on those discussions, the Presidency introduced a number of additional changes to address outstanding delegations' comments. Some further changes were introduced following a technical meeting with the European Parliament. For the ease of reference, the introduced changes are marked in bold underlined and listed below:

- unless specified below, the changes introduced in articles 1 and 3 are of a clarifying/streamlining nature;

- art. 1(6a) was amended to ensure that information exchanges with the Commission and other authorities should not only preserve confidentiality but also security and commercial interests of operators of essential services and digital service providers;

- in art. 3(12c) the definition of Domain Name System service provider was further improved;

- a recital linked to art. 3a(1) with regard to jurisdiction (FN 13) was amended to clarify the difference between entities and operators;

- a recital linked to art. 3a(2) on the list of services (FN 14) was amended not to prejudge which service are essential;

- the wording of art. 3a(3) was slightly simplified;

- the reference in art. 3a(4) was corrected.

- the deadline in art. 3a(6) was changed to 6 months.

- with regard to art. 5(1): the EP would like to set a deadline for the adoption of national NIS strategies. This is linked to art. 20a(1) and to the fact that the cooperation group should start working 6 months after entry into force and one of its tasks (art. 8a(3)(e)) is to evaluate national strategies. While the Presidency did not include this change in the text, it would like to retain flexibility, if needed during the trilogue, to propose a deadline between the transposition date and 6 months prior to the transposition date.

- the recital linked to art. 6(1) and (2a) proposed to address the European Parliament's concern that national competent authorities and single points of contact should not fulfil tasks in the fields of intelligence, law enforcement or defence was deleted at the request of majority of delegations. The Presidency is waiting for explanations from the European Parliament but expects that further discussions on how to deal with this issue will be needed.

- art. 7(1) on CSIRTs was amended to include both the sectors in Annex II and the types of DSPs in Annex III in the first subparagraph. In the Presidency's view it is now clear that one CSIRT can cover both.

- following the deletion of the word 'anonymised' in art. 6(4ab new) the same change was made in art. 8(3)(k) which refers to the same summary reports.

- a recital linked to Chapter IV on public administrations (FN 28) was further clarified.

- in art. 14(1a) the word 'ensure' was replaced by 'striving to mainain' with regard to the continuity of the service. This changes mirrors a similar change made previously in art. 15a(1a).

- art. 14(2c) on voluntary notification was reworded in an attempt to close this issue with the European Parliament.

- art. 14(6) it was reworded again in an attempt to close this issue with the European Parliament.

- in art. 15a a number of minor changes were introduced at the request of the European Parliament that wants to make clear that those provisions deal with services offered in the Union.

- a new recital was included in connection with art. 15a(1) concerning situations where operators of essential services rely on the service of a digital service provider.(FN 33)

- in art. 15a(2) the phrase 'after having become aware of it' was deleted at the request of several delegations.

- in art. 15c(2) it was clarified that the representative of providers not established in the Union, but offering services therein, shall be established in one of those Member States where the services are offered. The corresponding recital was aligned with the article.

- in art. 16(1) the reference to technological neutrality was replaced by a reference taken from recital 8 of the TSM Regulation.

- art. 16(1a) and (2) were amended in an attempt to find a compromise solution with the European Parliament which wants the Commision to adopt an implementing act with a list of standards on security requirements, the use of which should be encouraged by Member States. The text provided that the Commission shall take the ENISA advice and guidelines on this topic into account. Given the non-binding nature of any standards and the fact the use of them should merely be encouraged, the Presidency believes that it is possible to find an agreement with the Parliement here.

- art. 17 was aligned with the Joint Handbook for presentation and drafting of acts subject to the OLP agreed by the three institutions.

- art. 20a(1a) was further reworded to clarify the role of the cooperation group in the discussion of national measures and, when requested by a Member State, also of draft national measures. The timeline for this discussion was amended to fit better with the logic of the provision.

- with regard to Annex II a number of references were improved or corrected. In addition, the definitions in the fields of air, rail and water transports were amended to clarify that they include logistical services.

- since the European Parliament insists on the inclusion of ancillary logistical services for road transport, the Presidency proposed to include operators of intelligent transport systems instead as a compromise.

- in Annex III the definitions of online market place and of cloud have been amended.

5. The Coreper mandate (doc. 14606/1/15 REV 1) was discussed at the WP TELE of 2 December and, based on the delegations' comments, the following changes were introduced in the 4-column document:

- in the first recital related to art. 1(7) (FN 7) the last sentence has been deleted.

- the new recital related to art. 3a(1) (FN 13) has been deleted.

- the new recital related to art. 15a(2) (FN 34) has been deleted since a new paragraph 2a on incidents having a substantial impact has been included in art. 15a.

- in art. 15a, new paragraph 2b on situations where an operator of essential services relies on a third-party cloud computing service have been included.

- art. 16(2) has been deleted.

- the location of paragraph 2a in art. 21 has been corrected.

- operators of intelligent transport systems have been removed from Annex II.

6. In view of the next informal trilogue, and taking the above mentioned into account, the Presidency invites the Coreper to grant it a mandate on the basis of the text set out in the 3rd and 4th column of the attached 4-column document and in the separate table for Annex II.

_____

ANNEX

Proposal for a
Directive of the European Parliament and of the Council
concerning measures **with a view** to **achieving** ~~ensure~~ a high common level of network and information security across the Union

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Chapter I **GENERAL PROVISIONS**	**Chapter I** **GENERAL PROVISIONS**	**Chapter I** **GENERAL PROVISIONS**	**Chapter I** **GENERAL PROVISIONS**
Article 1	*Article 1*	*Article 1*	*Article 1*
Subject matter and scope	Subject matter and scope	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 **with a view** to **achieving** ~~ensure~~ a high common level of **security of** network**s** and information **systems** ~~security~~ (hereinafter referred to as "NIS") within the Union **so as to improve the functioning of the internal market.**	(no change since March)

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
1. To that end, this Directive:		2. To that end, this Directive:	(no change since March)
(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 **to adopt a national NIS strategy** ~~concerning the prevention, the handling of and the response to **serious** risks and incidents affecting networks and information systems~~;	
(a) creates a cooperation mechanism between Member States in order to ensure a uniform application of this Directive within the Union and, where necessary, a coordinated and efficient handling of and response to risks and incidents affecting network and information systems;	(b) creates a cooperation mechanism between Member States in order to ensure a uniform application of this Directive within the Union and, where necessary, a coordinated**,** ~~and~~ efficient ***and effective*** handling of and response to risks and incidents affecting network and information systems ***with the participation of relevant stakeholders***; (AM 40)	(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 and develop trust and confidence**~~ensure a uniform application of this Directive within the Union and, where necessary, a coordinated and efficient handling of and response to risks and incidents affecting network and information systems~~;	(b) creates a cooperation **group** in order to **support and facilitate strategic cooperation and the exchange of information among Member States and develop trust and confidence <u>amongst them</u>**;

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		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;	**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~~,~~ and effective operational cooperation**;
(b) establishes security requirements for market operators and public administrations.	(c) establishes security requirements for market operators. ~~and public administrations.~~ (AM 41)	(c) establishes security **and notification** requirements for ~~market~~ operators **of essential services** ~~and public administrations~~.	(c) establishes security and notification requirements for operators **of essential services ~~and for digital service providers~~**.
(c)			**(ca) establishes security and notification requirements for digital service providers.**
		d) lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of networks and information systems.	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
2. 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.**	3. The security and notification requirements provided for in **~~Articles 14 and 15a~~ this Directive** shall apply neither to undertakings which are subject to the requirements of Articles 13a and 13b of 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.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
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[1]		4. This Directive shall be without prejudice to **Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems, Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011on combating the sexual abuse and sexual exploitation of children and child pornography,** ~~EU laws on cybercrime and~~ **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.[2]	(no change since March)

1 OJ L 345, 23.12.2008, p. 75.
2 OJ L 345, 23.12.2008, p. 75.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
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[3], 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[4].	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.*** (AM 42)	No change	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[5], ~~**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**~~[6].

3 OJ L 281 , 23/11/1995 p. 31.
4 SEC(2012) 72 final.
5 OJ L 281 , 23/11/1995 p. 31.
6 ~~**SEC(2012) 72 final.**~~

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
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.		Note: moved to Article 1a(3a).	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		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.	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. **~~Such information shall be handled with due regard to its confidential nature.~~** **~~National authorities and the Commission shall respect the confidential nature of such information.~~** **Such exchange of information shall preserve the confidentiality of that information as well as the security and commercial interests of operators of essential services and digital service providers.**

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		6b. This Directive is without prejudice to the actions taken by Member States to safeguard their essential State functions, in particular to safeguard national security (including actions protecting information, the disclosure of which Member States consider contrary to the essential interests of their security), and to maintain law and order, in particular to permit the investigation, detection and prosecution of criminal offences.	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		7. If a sector specific Union legal act contains explicit obligations for operators to ensure either the ~~requirements for~~ security of networks and information systems ~~and/~~or ~~for~~ the notification of incidents, the provisions of that sector specific Union legal act shall apply instead of Article 14 of this Directive.	7. **~~If~~ Where** a sector specific Union legal act **~~contains~~ requires ~~explicit obligations for~~** operators **of essential services or digital service providers** to ensure either the security of **their** networks and information systems or the notification of incidents, **provided that such requirements are at least ~~comparable~~ equivalent in effect to the obligations contained in this Directive, ~~the~~ those** provisions of that sector specific Union legal act shall apply **~~in relation to those obligations such requirements~~ instead of ~~Article 14 and or 15a~~ the corresponding provisions of this Directive.**[7]

[7] To be accompanied by the following recitals:

(x) Certain sectors of the economy, including some of those referred to in Annex II, are already regulated or may be regulated in the future by sector specific Union legal acts that include rules related to the security of networks and information systems. Whenever those Union legal acts impose requirements concerning the security of networks and information systems or notifications of incidents, then these provisions should apply instead of the corresponding provisions of this Directive. In order for the sectoral Union legal acts to prevail they should contain requirements which are at least equivalent in effect to the obligations contained in this Directive. ~~Such legal acts should thus impose higher or more complex and specific obligations than those referred to in this Directive.~~

(x) Where a sector specific Union legal act defines the scope of entities subject to requirements concerning the security of networks and information systems or notification of incidents, then where this scope includes entities listed in sectors and subsectors as referred to in Annex

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	Article 1a	Article 1a	
	Protection and processing of personal data	*Protection and processing of personal data*	
	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.	**1. Processing of personal data pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC.**	(no change since March)
	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.	**2. Processing of personal data by Union institutions and bodies pursuant to this Directive 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.		

II, the Member States should apply the provisions of.this sector specific Union legal act, instead of carrying out the identification process for operators of essential services as defined by this Directive.

(x) Where the provisions of a sector specific Union legal act concerning the security of networks and information systems or notification of incidents apply instead of the corresponding provisions of this Directive it follows that the provisions concerning jurisdiction and supervision as set out in that sector specific Union legal act apply instead of the corresponding provisions of this Directive.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		3a. Processing of personal data, which is necessary to meet the objectives of public interest pursued by this Directive, is legitimate processing within the meaning of Article 7 of Directive 95/46/EC.	**~~3a. Processing of personal data, which is necessary to meet the objectives of public interest pursued by this Directive, is legitimate processing within the meaning of Article 7 of Directive 95/46/EC.~~**
	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. (AM 43)		

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Article 2	*Article 2*	*Article 2*	*Article 2*
Minimum harmonisation	Minimum harmonisation	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 **with a view to achieving** ~~ensure~~ a higher level of security **of networks and information systems**, without prejudice to their obligations under Union law.	(no change since March)

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Article 3	*Article 3*	*Article 3*	*Article 3*
Definitions	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:	(no change since March)
(1) "network and information system" means:		(1) "network and information system" means:	(no change since March)
(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	(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~~ ***digital*** data, as well as (AM 44)	(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** ~~computer~~ data, as well as	
(c) computer data stored, processed, retrieved or transmitted by elements covered under point (a) and (b) for the purposes of their operation, use, protection and maintenance.	c) ~~computer~~ ***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. (AM 45)	(c) **digital** ~~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.	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
(2) "security" means the ability of a network and information system to resist, at a given level of confidence, accident or malicious action that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system;	(2) 'security' means the ability of a network and information system to resist, at a given level of confidence, accident or malicious action that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system; ***'security' includes appropriate technical devices, solutions and operating procedures ensuring the security requirements set out in this Directive*** (AM 46)	(2) "security **of networks and information systems**" means the ability of ~~a~~ network**s** and information system**s** 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 **or processed** data or the related services offered by or accessible via that network and information system**s**;	(no change since March)

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		2a) "essential services" are services indispensable for the maintenance of critical societal and economic activities.	(deleted)
(1) "risk" means any circumstance or event having a potential adverse effect on security;	(3) 'risk' means any ***reasonably identifiable*** circumstance or event having a potential adverse effect on security; (AM 47)	(3) "risk" means any circumstance or event having a potential adverse effect on the security **of networks and information systems**;	(3) "risk" means any **reasonably identifiable** circumstance or event having a potential adverse effect on the security **of networks and information systems**;
(2) "incident" means any circumstance or event having an actual adverse effect on security;	(4) 'incident' means any ~~circumstance or~~ event having an actual adverse effect on security; (AM 48)	(4) "incident" means any circumstance or event having an actual adverse effect on **the** security **of networks and information systems;**	(4) "incident" means any ~~**circumstance or**~~ event having an actual adverse effect on **the** security **of networks and information systems;**
(5) "information society service" mean service within the meaning of point (2) of Article 1 of Directive 98/34/EC;	***Deleted*** (AM 49)	deleted	(no change since March)

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
(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	(no change since March)
		(6a) "National strategy on the security of networks and informations systems ("NIS strategy")" means a framework providing high-level vision, objectives and priorities on NIS at national level;	**(6a) "National strategy on the security of networks and informations systems ("NIS strategy")" means a framework providing ~~high-level vision,~~ strategic objectives and priorities on NIS at national level;**
(7) "incident handling" means all procedures supporting the analysis, containment and response to an incident;	(7) 'incident handling' means all procedures supporting the ***detection, prevention***, analysis, containment and response to an incident; (AM 50)	(7) "incident handling" means all procedures supporting the analysis, containment and response to an incident;	(no change since March)

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
(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;	***Deleted*** (AM 51)		
(b) operator of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health, a non exhaustive list of which is set out in Annex II.	(b) 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~~ ***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***	**(8) Operator means a public or private entity the type of which is referred to in Annex II, which provides an essential service in the fields of digital infrastructure, digital service platforms, energy, transport, banking, financial market infrastructures, health or drinking water and which fulfils all of the following criteria:**	(8) "operator **of essential services**" means a public or private entity the type of which is referred to in Annex II, which meet**s** the criteria laid down in Article 3a(1a) [8]

[8] **To be accompanied by the following recital :**

(x) This Directive applies to operators of essential services, the types of which are listed in the Annex II, and to digital service providers, providing services as referred to in Annex III. Such operators of essential services and digital service providers may be in public or private ownership. ~~Therefore, public administrations (at national, regional, and local levels) which are identified by Member States as operators of essential services pursuant to Article 3a(1), or which meet the definition of digital service provider set out in Article 3(8a), are subject to the provisions of this Directive in that regard.~~

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	core services; (AM 52)		
(c)		**- the service depends on network and information systems;**	Deleted – see new article 3a
		- an incident to the network and information systems of the service would have significant disruptive effects on the provision of that essential service or on public safety.	Deleted – see new article 3a
		Each Member State shall identify the entities, which meet the above definition of operator.	Deleted – see new article 3a
		When determining the significance of a disruptive effect, the Member State shall take into account the following factors:	Deleted – see new article 3b
		- the importance of the particular entity for the provision of the essential service in the sector;	Deleted – see new article 3b

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		- the number of users relying on the services provided by the entity;	Deleted – see new article 3b
		- the impact on economic and societal activities or public safety where the availability, authenticity, integrity or confidentiality of the service provided by the entity has been compromised, including assessment of the time period before discontinuity would create a negative impact.	Deleted – see new article 3b
	(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; (AM 53)		
			(8a) 'digital service provider' means any legal person that provides an information society service within the meaning of point (2) of Article 1 of Directive 98/34/EC **offered to the public at large or to businesses at large,** and the type of which is listed in Annex III.[9]

[9] **To be accompanied by the same recital as Article 3(8):**

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
(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;	(no change since March)
(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;	(no change since March)
(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		(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~~.	**~~(11) "Trust service provider" means a natural or legal person within the meaning of point (19) of Article 3 of Regulation 910/2014.~~**

(x)This Directive applies to operators of essential services, the types of which are listed in the Annex II, and to digital service providers, providing services as referred to in Annex III. Such operators of essential services and digital service providers may be in public or private ownership. ~~Therefore, public administrations (at national, regional, and local levels) which are identified by Member States as operators of essential services pursuant to Article 3a(1), or which meet the definition of digital service provider set out in Article 3(8a), are subject to the provisions of this Directive in that regard.~~

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
seals.			
			(12a) "representative" means any natural or legal person established in the Union explicitly designated to act on behalf of a digital services provider not established in the Union, which may be addressed by the competent authority or CSIRT instead of the digital service provider, with regard to the obligations of the digital service provider under this Directive.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			(12b) "Internet Exchange Point (IXP) " means a ~~physical location where a number of public communications networks can exchange internet traffic with each other~~[10] network facility that enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of Internet traffic. An IXP provides interconnection only for autonomous systems. An IXP does not require the Internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic.[11]

~~To be accompanied by the following recital:~~

~~(x) **It is important to make the distinction** between the different categories of Internet Exchange Points in particular between those who are facilitating the exchange of aggregated internet traffic between multiple network operators and those who are single network operators which physically interconnect their networks based on an interconnection agreement. In the latter case, the network providers are covered by the security obligations laid down in Article 13a of the Framework Directive.~~

[11] To be accompanied by the following recital

The function of an IXP is to interconnect networks. An IXP does not provide network access or act as a transit provider or carrier. An IXP also does not provide other services unrelated to interconnection (although this does not preclude an IXP operator from also providing unrelated services). An IXP exists to interconnect networks that are technically and organisationally separate. The term autonomous system is used to describe a technically stand-alone network.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			(12c) "Domain Name System **service provider**" means **an ~~operator~~ entity which ~~contributes to the internet~~ provides DNS services on the internet (DNS is a hierarchical distributed naming system in a network which refers queries for domain names ~~for computers, services or any other resource connected to Internet or to a private network which enables the association of domain names with various kinds of information, in particular IP (Internet Protocol) addresses.~~)**
			(12d) "Top-level domain name registry" means an entity which ~~designated to~~ ~~administrate~~ administers and ~~manage~~ operates the registration of internet domain names under a specific Top-level domain (TLD), ~~including the encoding of TLD names into IP addresses.~~

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	(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).*** (AM 54)	Note: the wording of this provision shall be finalised pending further information from the Commission on NIS requirements in sector-specific legislation (point 4 of Annex II).	See Annex II
	(11b) 'multilateral trading facility (MTF)' means multilateral trading facility as defined in point 15 of Article 4 of Directive 2004/39/EC; (AM 55)	Note: the wording of this provision shall be finalised pending further information from the Commission on NIS requirements in sector-specific legislation (point 4 of Annex II).	See Annex II

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	(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; (AM 56)	Note: the wording of this provision shall be finalised pending further information from the Commission on NIS requirements in sector-specific legislation (point 4 of Annex II).	See Annex II

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			Article 3a
			Identification of operators **of essential services** ~~in the sectors referred to in Annex II~~
			1. **~~By (…) 6 months after the date set out in Article 21(1), f~~F**or each subsector referred to in Annex II, Member States shall identify **the** operators **of essential services on their territory**.[12] [13]

[12] To be accompanied by the following recitals:

(x) Member States should be responsible for determining which entities meet the criteria of the definition of operator of essential services as part of the transposition- of the Directive into national law. In order to ensure a consistent approach, the definition of operator **of essential services** should be coherently applied by all Member States. ~~A common methodology~~ **For this purpose the Directive provides for ~~should consist of~~** the assessment of the entities active in the subsectors, or in the sector where no subsector is listed in Annex II, the ~~requirement to~~ establish**ment of** a list of essential services, the consideration of a common list of cross-sectoral ~~and [sectoral]~~ factors to determine whether a potential incident would have a significant disruptive effect, a consultation process involving relevant Member States in case of entities providing services in more than one Member State, and the support of the Cooperation Group in the identification process. In order to ensure that the scope reflects possible changes in the market, the list of identified operators should be reviewed regularly by Member States and updated when necessary. Finally Member States should submit to the Commission the information necessary to assess the extent to which this common methodology allowed a consistent application of the definition by Member States.

(x) In the process of identification **of operators of essential services**, Member States should **assess**, at least for each subsector referred to in Annex II, **which** services **have to be** considered **as** essential for the maintenance of critical societal and economic activities and assess whether the entities **listed** in Annex II **and providing those services** meet the three criteria for the identification of operators. When assessing the first criterion, it is sufficient to examine whether a specific entity provides an essential service that is included in the list of services. When assessing the second criterion, it is necessary to demonstrate that provision of the essential service is dependent on network and information systems. When assessing the third criterion, Member States should take into account a number of cross-sectoral factors.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			1a. The criteria referred to in Article 3(8) shall be as follows :
			(a) an entity provides a service which is essential for the maintenance of critical societal and/**or** economic activities;
			(b) the provision of that service depends on network and information systems; and
			(c) an incident to the network and information systems of that service would have significant disruptive effects on its provision~~**or on public safety**~~.

[13] Following clarifying recital could be included with regard to jurisdiction:
(x) ~~**Member States should identify entities as operators of essential services on their territory. The entities in the sectors listed in Annex II are of different types and Member States should identify operators having due regard to the nature of the service. In the case of physical infrastructure such as airports, ports, and oil storage refinement facilities, Member States should consider operators of such facilities located on their territory; in the case of service providers such as airlines they should consider those established in their territory, but not other airlines serving an airport located in their territory; in the case of DNS service providers they should consider those established in their territory.**~~
~~**When a Member State receives a service it considers essential delivered by an entity located on the territory of another Member State, the competent authority of that Member State shall inform the competent authority of the other Member State about the essential nature of the service provided. The Member State where the operator is located shall as a consequence identify that entity as an essential operator which shall fall within its jurisdiction, even if that entity doesn't deliver an essential service to that Member State.**~~

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			2. For the purposes of paragraph 1, Member States shall establish a list of **the** services referred to in point (a) of paragraph 1a.[14]

[14] To be accompanied by the following recital:

(x) ~~Operators~~ **Entities ~~listed~~** in the sectors and subsectors **listed ~~of~~ in** Annex II may provide essential and non-essential services. For example, in the air transport sector, airport**s may** provide ~~**essential**~~ services**, which might be considered by a Member State as essential,** such as the management of the runways, but also a number of services which **~~are~~ might be considered** as non-essential, such as the provision of shopping areas. Operators **of essential services** should be subject to the specific security obligations only with respect to those services~~,~~ which are deemed essential. For the purpose of identifying operators, Member States ~~shall~~ **should** therefore establish a list of **the** services which are considered as essential.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			3. For the purposes of paragraph 1, **where ~~a Member State intends to decide on the identification of an entity and that~~** an entity provides a service referred to in point (a) of paragraph 1a in ~~several~~ **two or more** Member States, **those ~~that~~** Member State**s** shall engage in consultation with **each ~~those~~ other ~~Member States~~. That consultation shall take place before a decision on the identification ~~of that operator of essential services~~ is taken.**[15]

[15] To be accompanied by the following recital:

(x) **~~Where a Member State ascertains during the identification process that a potential operator provides the essential service also in other Member States, the identifying that Member State should inform the other Member States concerned and . The identifying Member State should engage in bilateral and/or multilateral discussions with the other Member States concerned them.~~ For the purposes of the identification process, where a potential operator provides the essential service in two or more Member States, those Member States should engage in bilateral and/or multilateral discussions with each other.** This consultation process is intended to help Member States to assess the criticality of the operator in terms of cross-border impact and allows each Member State involved to present its views regarding the risks associated to the services provided by the operator. In this process Member States concerned should take into account each other's views. The Member States concerned may request the assistance of the Cooperation Group in this regard.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			4. Member States shall on a regular basis, and at least every two years after the date referred to in **~~paragraph 1~~ Article 21(1)~~(2)~~**, review and**, where appropriate,** update the list of identified operators **of essential services**.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			5. The role of the Cooperation Group shall be, ~~**within the limits of**~~ **in accordance with** the tasks referred to in Article 8a, to support Member States **to take a consistent approach** in the process of identification of operators **of essential services**.
			6. For the purpose of the review referred to in Article 20 and by (...) (~~**one year**~~ **6 months** after the date of transposition), and every ~~**second**~~ **two** year**s** thereafter, Member States shall submit to the Commission the information necessary for the Commission to assess the implementation of this Directive, in particular the consistency of Member States' approaches to the identification of operators **of essential services**. That information shall include at least:

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			(a) national measures allowing for the identification of operators **of essential services**;[16]
			(b) ~~a~~ **the** list of services referred to in paragraph 2;
			(c) the number ~~**and the proportion**~~ of operators **of essential services** identified for each sector referred to in Annex II **and an indication of their importance** ~~**part of the**~~ **in relation to that sector** ~~**that they represent**~~;[17]

[16] To be accompanied by the following recital:
(x) As a result of the identification process Member States should adopt national measures which will ~~**unequivocally**~~ determine which entities are subject to NIS obligations. This result could be achieved by adopting a list enumerating all operators of essential services or by adopting national measures including objective quantifiable criteria (e.g. output of the ~~**company**~~ **operator** or number of users) which would allow to determine which entities are in the scope and which are not. The national measures should include all ~~**policies and**~~ legal measures, **administrative measures and policies** allowing for the identification of operators of essential services under this Directive, whether already existing or adopted in the context of this Directive.

[17] To be accompanied by the following recital :
In order to give an indication of the importance of the identified operators in relation to the sector concerned, Member States should take into account the number and the size of identified operators, for example in terms of market share or of the quantity produced or carried, without being obliged to divulge information which would reveal which operators have been identified.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			(d) thresholds, where they exist, to determine the relevant supply level in accordance with the number of ~~parties~~ **users** relying on that service in accordance with point (~~c~~**a**) of Article 3b or the importance of that particular operator **of essential services** in accordance with point (f) of Article 3b.
			In order to contribute to the provision of comparable information, the Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical guidelines on parameters for the information referred to in this paragraph.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			Article 3b
			Significant disruptive effect
			1. When determining the significance of a disruptive effect referred to in point (c) of Article 3a(1a), Member States shall take into account **at least** the following cross-sectoral factors:
			(a) the number of users[18] relying on the service~~s~~ provided by the entity;
			(b) the **direct** dependency of other sectors in Annex II on the service provided by the entity;

[18] To be accompanied by the following recital:

(x) For the purpose of determining the significance of a disruptive effect of an incident on an essential service, Member States should take into account the number of natural persons ~~or~~ **and** legal entities using that service for private or professional purposes. The use of that service can be direct, indirect or by intermediation

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			(c) the impact ~~of~~ **that** incidents **could have,** in terms of degree and duration**,**[19] on economic and societal activities or public safety;
			(d) the market share of the entity;
			(e) the geographic spread with regard to the area that could be affected by an incident;
			(f) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternatives for the provision of that service;

19 To be accompanied by the following recital:

(x) For the purpose of determining the significance of a disruptive effect of an incident, Member States should take into account the severity of the consequences of a potential incident on economic and societal activities or public safety as well as the duration of such effects, the time period until the incident would produce its negative effects and the expected time needed to restore the normal functioning of the service.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			2. In order to determine whether an incident would have a significant disruptive effect, Member States shall also take into account sector-specific factors where appropriate[20]**.**

[20] To be accompanied by the following recital:
(x) In order to determine whether an incident would have a significant disruptive effect on the provision of a service**,** in addition to the cross-sectorial factors, sector specific factors should also be considered**.** With regard to energy suppliers such factors could include the volume or proportion of national power generated; for oil suppliers the volume per day; for air transport (including airports and air carriers), rail transport and maritime ports the proportion of national traffic volume and the number of passengers or cargo operations per year; for banking/financial market infrastructures their systemic importance based on total assets or the ratio of those total assets to GDP; for health, the number of patients under the provider's care per year; for water production, processing and supply the volume and number and types of users supplied (including for instance hospitals, public service, organisations or individuals), and the existence of alternative sources of water to cover the same geographical area; ~~**For the purpose of the review of this Directive, Member States should also submit to the Commission any relevant thresholds used in the context of these sector-specific factors.**~~

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Chapter II NATIONAL FRAMEWORKS ON NETWORK AND INFORMATION SECURITY			**Chapter II** **NATIONAL FRAMEWORKS ON NETWORK AND INFORMATION SECURITY**
Article 4	*Article 4*	*Article 4*	
Principle	Principle	Principle	
Member States shall ensure a high level of security of the network and information systems in their territories in accordance with this Directive.	Deleted	Deleted	(no change since March)

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Article 5	*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~~***	***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 **with a view** to achiev**eing** and maintain**ing** a high level of **security of** networks and information **systems** ~~security~~ **at least in the fields referred to in Article 3(8)**. 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~~ **and appopriate policy and regulatory measures** with a view to achieving and maintaining a high level of security of networks and information systems **and covering at least the sectors referred to in Annex II and the services referred to in Annex III**. **~~The national NIS strategy shall also include concrete policy and regulatory measures at least in for the fields referred to in Article 3(8) the sectors referred to in Annex II.~~** 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~~ objectives and priorities of the **national NIS** strategy~~ based on an up-to-date risk and incident analysis~~;	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
(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) A governance framework 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**;	
(e) Research and development plans and a description of how these plans reflect the identified priorities.		(e) **An indication of the r**esearch~~-~~and development plans **relating to the NIS strategy** ~~and a description of how these plans reflect the identified priorities~~;	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	(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. (AM 57)		
2. The national NIS strategy shall include a national NIS cooperation plan complying at least with the following requirements			
(a) A risk assessment plan to identify risks and assess the impacts of potential incidents;	a) A risk ~~assessment plan to identify risks and assess~~ ***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***; (AM 58)	(f) A risk assessment plan to identify **possible**-risks ~~and assess the impacts of potential incidents~~;	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
(b) The definition of the roles and responsibilities of the various actors involved in the implementation of the plan;	(b) The definition of the roles and responsibilities of the various ***authorities and other*** actors involved in the implementation of the ~~plan~~ ***framework***; (AM 59)	(g) ~~The definition of the roles and responsibilities~~ **A list** of the various actors involved in the implementation of the **NIS strategy** ~~plan~~;	
(c) The definition of cooperation and communication processes ensuring prevention, detection, response, repair and recovery, and modulated according to the alert level;			
(d) A roadmap for NIS exercises and training to reinforce, validate, and test the plan. Lessons learned to be documented and incorporated into updates to the plan.			

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		2a. Member States may request the assistance of ENISA in developing national NIS strategies. For the purposes of this paragraph, ENISA shall act within the limits of its mandate set out in Articles 2 and 3 of Regulation 526/2013.	**2a. Member States may request the assistance of ENISA in developing national NIS strategies. ~~For the purposes of this paragraph, ENISA shall act within the limits of its mandate set out in Articles 2 and 3 of Regulation 526/2013.~~**
3. The national NIS strategy and the national NIS cooperation plan shall be communicated to the Commission within one month from their adoption.	3. The national NIS strategy and the national NIS cooperation plan shall be communicated to the Commission within ~~one month~~ ***three months*** from their adoption. (AM 60)	3. **The Member States shall make available to the Commission at least a summary of** the national NIS strategy ~~and the national NIS cooperation plan shall be communicated to the Commission within one month from their adoption~~ within ~~one month~~ **three** month**s** from their adoption.	3. ~~**The Member States shall make available to the Commission at least a summary of t**~~**T**he national NIS strategy ~~and the national NIS cooperation plan~~ **shall be communicated to the Commission** ~~within one month from their adoption~~ within ~~one month~~ **three** month**s** from ~~**their**~~ **its** adoption. **In so doing, Member States may exclude elements of the strategy related to national security.**

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Article 6	*Article 6*	*Article 6*	*Article 6*
National competent authority on the security of network and information systems	National competent ~~authority~~ ***authorities and single points of contact*** on the security of network and information systems (AM 61)	**National competent authorities~~y~~ and single point of contact**	**National competent authorities~~y~~ and single point of contact.**[21]
1. Each Member State shall designate a national competent authority on the security of network and information systems (the "competent authority").	1. Each Member State shall designate ~~a~~ ***one or more civilian*** national competent ~~authority~~ ***authorities*** on the security of network and information systems (***hereinafter referred to as*** ~~the~~ 'competent authority***/ies***'). (AM 62)	1. Each Member State shall designate **one or more** ~~a~~ national competent authorit**ies**~~y~~ on the security of network and information systems (the "competent authority"). **Member States may designate this role to an existing authority or authorities.**	1. Each Member State shall designate **one or more** ~~a~~ national competent authorit**ies**~~y~~ on the security of network and information systems (the "competent authority") **covering at least the sectors refered to in Annex II and the digital services referred to in Annex III**. **Member States may designate this role to an existing authority or authorities**
2. The competent authorities shall monitor the application of this Directive at national level and contribute to its consistent application throughout the Union.		2. The competent authorities shall monitor the application of this Directive at national level ~~and contribute to its consistent application throughout the Union~~.	(no change since March)

[21] ~~**To be accompanied by the following recital:**~~
~~**(x) Member States should remain free to organise their competent authorities and single points of contact, while having in mind that preference should be given to structures which do not fulfil any tasks in the field of intelligence, law enforcement or defence.**~~

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	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. (AM 63)	**2a. Each Member State shall designate one or more national single points of contact on the security of networks and information systems ("single point of contact"). Member States may designate this role to an existing authority. Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact.**	**2a. Each Member State shall designate ~~one or more~~ a national single points of contact on the security of networks and information systems ("single point of contact"). Member States may designate this role to an existing authority. Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact.**
	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. (AM 64)	[covered in 7(1a)]	(no change since March)

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	2c. The single point of contact shall ensure cross-border cooperation with other single points of contact. (AM 65)	**2c. With a view to the transparent functioning of the cooperation group and the CSIRTs network, the single point of contact shall exercise a liaison function between its Member State and the cooperation group and the CSIRTs network.**	**2c. ~~With a view to the transparent functioning of the cooperation group and the CSIRTs network, t~~The single point of contact shall exercise a liaison function ~~between its~~ to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the cooperation group and the CSIRTs network.**
3. Member States shall ensure that the competent authorities have adequate technical, financial and human resources to carry out in an effective and efficient manner the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure the effective, efficient and secure cooperation of the competent authorities via the network referred to in Article 8.	3. Member States shall ensure that the competent authorities ***and the single points of contact*** have adequate technical, financial and human resources to carry out in an effective and efficient manner the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure the effective, efficient and secure cooperation of the ~~competent authorities~~ ***single points of contact*** via the network referred to in Article 8. (AM 66)	3. Member States shall ensure that the **relevant** 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 competent authorities via~~ **in** the ~~network~~ **cooperation group and the CSIRTs network** referred to in Articles 8**a and 8b**.	3. Member States shall ensure that the ~~relevant~~ **designated** 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 competent authorities via~~ **of the designated representatives in** the ~~network~~ **cooperation group ~~and the CSIRTs network~~** referred to in Articles~~s~~ 8**a ~~and 8b~~**.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
4. Member States shall ensure that the competent authorities receive the notifications of incidents from public administrations and market operators as specified under Article 14(2) and are granted the implementation and enforcement powers referred to under Article 15.	4. Member States shall ensure that the competent authorities ***and single points of contact, where applicable in accordance with paragraph 2a of this Article,*** 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 (AM 67)	4. Member States shall ensure that the competent authorities **or CSIRTs** receive the notifications of incidents from ~~market~~ operators **of essential services** as specified under Article 14(2) **and 14(2ac)** ~~and are granted the implementation and enforcement powers referred to under Article 15~~.	4. Member States shall ensure that the competent authorities or CSIRTs receive the notifications of incidents ~~from operators of essential services~~ as specified under Article 14(2), ~~and~~ 14(2ac) **and 15a(2)**.[22]
		4a (new) In order to enable the single points of contact to submit a summary report on notifications to the Cooperation Group, Member States shall ensure that the competent authorities inform the single points of contact about notifications of incidents under Article 14(2) and 14(2ac) where the incident has a significant cross-border impact.	4a (new) In order to enable the single points of contact to submit a summary report on notifications to the Cooperation Group, Member States shall ensure that the competent authorities **or CSIRTs** inform the single points of contact about notifications of incidents under Article 14(2), ~~and~~ 14(2ac) **and 15a(2)** ~~**where the incident has a significant cross-border impact**~~**.**

[22] To be accompanied by the following recital:
Competent authorities or CSIRTs should receive the notifications of incidents. The single points of contact should not receive directly any notifications of incidents unless they also act as a competent authority or CSIRT. A competent authority or CSIRT might however task the single point of contact to forward incident notifications to the single points of contact of other affected Member States.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			4ab (new) Once a year, the **single point of contact** ~~competent authority~~ shall submit **~~an anonymised~~**[23] summary report to the cooperation **group** ~~network~~ on the notifications received, **including the number ~~and the nature~~ of notifications and the nature of notified incidents,** and the action taken in accordance with ~~this~~ **~~paragraphs~~ article 14(2), 14 (2ac) and 15a(2).** ~~paragraph~~.

[23] To be accompanied by the following recital :
The summary report submitted by the single point of contact to the cooperation group should be anonymised in order to preserve the confidentiality of the notifications and the identity of operators of essential services and DSPs as information on the identity of the notifying entities is not required for the exchange of best practices in the cooperation group. The summary report should include information on the number of notifications received, as well as an indication on the nature of the notified incidents, such as the types of security breaches, their seriousness or their duration.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	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.(AM 68)		

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
5. The competent authorities shall consult and cooperate, whenever appropriate, with the relevant law enforcement national authorities and data protection authorities.	5. The competent authorities ***and single points of contact*** shall consult and cooperate, whenever appropriate, with the relevant law enforcement national authorities and data protection authorities. (AM 69)	5. The competent authorit~~yies~~ **and single point of contact** shall, **whenever appropriate and in accordance with national legislation,** consult and cooperate, ~~whenever appropriate,~~ with the relevant **national** law enforcement ~~national~~ authorities and data protection authorities.	5. The competent authorities and single point of contact shall, whenever appropriate and in accordance with national ~~legislation~~ **law ~~complying with Union law~~**, consult and cooperate, whenever appropriate, with the relevant national law enforcement authorities and **national** data protection authorities.
6. Each Member State shall notify to the Commission without delay the designation of the competent authority, its tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent authority.	6. Each Member State shall notify to the Commission without delay the designation of the competent ~~authority~~ ***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 ~~authority~~ ***authorities***. (AM 70)	6. Each Member State shall notify to the Commission without delay the designation of the competent authority **and single point of contact, their** ~~its~~ tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent authority **and single point of contact.** **The Commission shall publish the list of designated single points of contacts.**	(no change since March)

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Article 7	*Article 7*	*Article 7*	*Article 7*
Computer Emergency Response Team	Computer Emergency Response Team	**Computer Security Incident ~~Emergency~~ Response Teams**	**Computer Security Incident 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.	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. (AM 71)	1. Each Member State shall **designate one or more** ~~set up a~~ Computer **Security Incident** ~~Emergency~~ Response Teams (hereinafter: "**CSIRTs** ~~CERTs~~") **covering at least the fields set out 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 **CSIRT** may be established within the competent authority.	1. Each Member State shall designate one or more Computer Security Incident Response Teams (hereinafter: "CSIRTs ") covering at least the **sectors referred to** in Annex II **and types of digital service providers referred to in Annex III,** 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**~~ **a** competent authority. ~~**Member State may shall also designate one or more CSIRTs covering the digital services referred to in Annex III.**~~

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		1a. Where they are separate, the competent authority, the single point of contact and the CSIRTs of the same Member State shall cooperate with regard to the obligations laid down in this Directive. Where a Member State decides that CSIRTs shall not receive notifications, the CSIRTs may, to the extent necessary to fulfil its tasks, be granted access to data on incidents notified by operators **of essential services** pursuant to Article 14(2) and (2ac).	1a. Where they are separate, the competent authority, the single point of contact and the CSIRTs of the same Member State shall cooperate with regard to the obligations laid down in this Directive. Where a Member State decides that CSIRTs shall not receive notifications, the CSIRTs ~~may~~ **shall**, to the extent necessary to fulfil ~~its~~ **their** tasks, be granted access to data on incidents notified by operators **of essential services** pursuant to Article 14(2) and (2ac) **or by digital service providers pursuant to Article 15a(2)**.
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 **the designated CSIRTs** ~~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 the designated CSIRTs have adequate resources to effectively carry out their tasks set out in point (2) of Annex I. **Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRT network referred to in Article 8b.**

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
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 **the designated 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~~.	3. Member States shall ensure that the designated CSIRTs have access to an appropriate, **secure, and resilient** communication and information infrastructure at national level
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~~.	4. Member States shall inform the Commission about the remit **including general information on the incident handling process** of the CSIRTs.
GREEN: agreed in principle (5.12.14) Deleted	5. The CERT***s*** shall act under the supervision of the competent authority ***or the single point of contact***, which shall regularly review the adequacy of ~~its~~ ***their*** resources, ~~its~~ ***mandates*** and the effectiveness of ~~its~~ ***their*** incident-handling process. (AM 72)	deleted	(no change since March)

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	5a. Member States shall ensure that CERTs have adequate human and financial resources to actively participate in international, and in particular Union, cooperation networks. (AM 73)		
	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. (AM 74)		
	AM75 ***5c. Member States may ask for the assistance of ENISA or of other Member States in developing their national CERTs.***	**5c. Member States may request the assistance of ENISA in developing national CSIRTs. For the purposes of this paragraph, ENISA shall act within the limits of its mandate set out in Articles 2 and 3 of Regulation 526/2013.**	5c. Member States may request the assistance of ENISA in developing national CSIRTs. ~~**For the purposes of this paragraph, ENISA shall act within the limits of its mandate set out in Articles 2 and 3 of Regulation 526/2013.**~~

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
CHAPTER III COOPERATION BETWEEN COMPETENT AUTHORITIES			**CHAPTER III** **COOPERATION BETWEEN COMPETENT AUTHORITIES**
Article 8	Article 8	~~Article 8~~	
Cooperation network	Cooperation network	~~Cooperation network~~	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		Article 8a	
		Cooperation group ~~network~~	
		1. In order to support and facilitate strategic cooperation among Member States, to develop trust and confidence and with a view to achieving a high common level of security of networks and information systems in the Union, a cooperation group is hereby established. **The cooperation group shall carry out its tasks on the basis of ~~a~~ biennial work programmes ~~roadmap~~ as referred to in Article 8a(3a new).**	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		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, the cooperation group may invite representatives from the relevant stakeholders to participate in its work[24].**	(no change since March)
		3. The cooperation group shall have the following tasks:	(no change since March)

[24] Recital to be added to specify what "relevant stakeholders" is deemed to encompass. Include specifically operators and providers of cybersecurity solutions.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		a. By [insert date, linked to entry into force] and every one and a half year[s] thereafter, establish a roadmap on actions to be undertaken to implement the objectives and tasks, which shall be consistent with the objectives of this Directive[25].	a. By [~~insert date, linked to entry into force~~ **18 months after entry into force**] and every ~~one and a half~~ **two** year~~[s]~~ thereafter, establish a ~~roadmap~~ **work programme** on actions to be undertaken to implement the objectives and tasks, which shall be consistent with the objectives of this Directive[25]
		b. Provide strategic guidance for the activities of the CSIRTs network established under Article 8b.	
		c. Exchange best practice on the exchange of information related to incident notification referred to in Article 14(2ac).	c. Exchange best practice on the exchange of information related to incident notification referred to in Article 14(2ac) **and 15a(2)**.

[25] Recital to be added to specify that the work programme should be consistent with the Union's legislative and policy priorities in the area of NIS.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		d. Exchange best practices between Member States and, in collaboration with ENISA, assist Member States in building capacity in NIS.	
		e. Discuss capabilities and preparedness of the Member States, and, on a voluntary basis, evaluate national NIS strategies and the effectiveness of CSIRTs, and identify best practices.	
		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.	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		h. Where relevant, exchange experiences on matters concerning NIS with relevant Union bodies, offices and agencies. [26]	

[26] To be accompanied by the following recital:

In order to promote advanced network and information security ~~To ensure that it fully achieves its objectives~~, the cooperation group should, **where relevant, cooperate** ~~liaise~~ with relevant **Union institutions**, bodies**, offices and agencies, ~~including the European Cybercrime Centre within Europol and Union data protection authorities~~**, to exchange know-how and best practices and to provide advice on NIS aspects that might have an impact on their work, **while respecting existing arrangements for the exchange of restricted information**. ~~The cooperation group should aim to achieve synergies between the efforts of those bodies and its own efforts to promote advanced network and information security~~. **[**In **cooperating** liaising with law enforcement bodies regarding network and information security aspects that might have an impact on their work, the cooperation group should respect existing channels of information and established networks.**]**

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		i. Discuss, with representatives from the relevant European Standardisation Organisations, the standards referred to in Article 16.	
		j. Collect best practice information on risks and incidents affecting network and information systems;	
		k. Examine on an annual basis the anonymised summary reports referred to in Article 14 (4).	k. Examine on an annual basis the **anonymised** summary reports referred to in Article **~~14 (4)~~6(4ab new)**.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		l. Discuss the work undertaken with regard to NIS exercises, education programmes and training, including the work by ENISA.	
		m. With ENISA´s assistance, exchange best practices with regard to the identification of operators **of essential services** by the Member States, including in relation to cross-border dependencies regarding NIS risks and incidents.	
		n. Discuss modalities for reporting notifications of incidents referred to in Article 14.	n. Discuss modalities for reporting notifications of incidents referred to in Article 14 **and 15a**.
		4. As input to the Commission's periodic review of the functioning of this Directive, the cooperation group shall every one and a half years years produce a report assessing the experience gained with the strategic cooperation pursued under this Article.	(no change since March)

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
4. The Commission shall establish, by means of implementing acts, the necessary modalities to facilitate the cooperation between competent authorities and the Commission referred to in paragraphs 2 and 3. Those implementing acts shall be adopted in accordance with the consultation procedure referred to in Article 19(2).	4. The Commission shall establish, by means of implementing acts, the necessary modalities to facilitate the cooperation between ~~competent authorities and~~ ***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 ~~consultation~~ ***examination*** procedure referred to in Article 19~~(2).~~ (***3***). (AM 80)	5. The Commission, taking the views of ENISA into account, shall establish 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).	5. **By [6 months after entry into force]** ~~T~~**t**he Commission, taking the views of ENISA into account, shall establish 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~~**3**).

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		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, a network of the national CSIRTs is hereby established.	(no change since March)
		2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT-EU. The Commission shall participate in the CSIRTs network as an observer. The European Network and Information Security Agency (ENISA) shall provide the secretariat ~~functions~~ and actively support the cooperation among the CSIRTs.	
		3. The CSIRTs network shall have the following tasks:	
		a. Exchange information on CSIRTs services, operations and cooperation capabilities.	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		b. At the request of a Member State potentially affected by an incident, exchange and discuss non-commercially sensitive information related to that incident and associated risks. Any Member State may refuse to contribute to that discussion if there is a risk of prejudice to the investigation of the incident.	**b. At the request of the representative of a Member State potentially affected by an incident, exchange and discuss non-commercially sensitive information related to that incident and associated risks. Any Member State may refuse to contribute to that discussion if there is a risk of prejudice to the investigation of the incident.**
		c. Exchange and make available on a voluntary basis non-confidential information on individual incidents.[27]	
		d. At the request of the representative of the Member State's CSIRT, discuss and, where possible, identify a coordinated response to an incident that has been identified within the jurisdiction of that same Member State.	**d. At the request of the representative of ~~the~~ a Member State's CSIRT, discuss and, where possible, identify a coordinated response to an incident that has been identified within the jurisdiction of that same Member State.**

[27] Proposal for a recital by Commission: "Information about NIS incidents is increasingly valuable to the general public and businesses, particularly small and medium-sized businesses. In some cases, such information is already provided via websites at the national level, in the language of a specific country and focusing mainly on incidents and occurrences with a national dimension. Given that businesses increasingly operate cross-border and citizens use online services, information on incidents should be provided in an aggregated form at EU level. The secretariat of the CSIRT network should maintain a website or host a dedicated page on an existing website where general information on major NIS incidents occurring across the Union is put at the disposal of the general public, with a specific focus on the interests and needs of businesses. CSIRTs participating in the CSIRTs network should provide the information to be published in this website. This website should not include confidential or sensitive information."

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		e. Support Member States in adressing cross-border incidents on the basis of their voluntary mutual assistance.	
		f. Discuss, ~~and~~ explore and identify further forms of operational cooperation, including ~~as regards~~ in relation to:	
		(i) categories of risks and incidents	
		(ii) early warnings	
		(iii) mutual assistance	
		(iv) principles and modalities for coordination, when Member States respond to cross border NIS risks and incidents.	
		g. Inform the Cooperation Group on its activities and on the further forms of operational cooperation discussed pursuant to paragraph 3(f), and request guidance related thereto.	
		h. Discuss lessons learnt from NIS exercises, including from those organised by ENISA.	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		i. At the request of an individual CSIRT, discuss the capabilities and preparedness of that same CSIRT.	
		j. Issue guidelines in order to facilitate the convergence of (operational) practices with regard to the application of the provisions of this Article concerning operational cooperation.	
		4. As input to the Commission's periodic review of the functioning of this Directive, the CSIRTs network shall every one and a half years produce a report assessing the experience gained with the operational cooperation, including conclusions and recommendations, pursued under this article. That report shall als be submitted to the cooperation group.	
		5. The CSIRTs network shall define its own rules of procedure.	(no change since March)

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Article 9	*Article 9*	~~*Article 9*~~	
Secure information-sharing system	Secure information-sharing system	~~Secure information-sharing system~~	
Deleted with some provisions accommodated in articles 8a/8b			

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Article 10	Article 10	~~Article 10~~	
Early warnings	Early warnings	~~Early warnings~~	
Deleted with some provisions accommodated in articles 8a/8b			

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Article 11	Article 11	~~Article 11~~	
Coordinated response	Coordinated response	~~Coordinated response~~	
Deleted with some provisions accommodated in articles 8a/8b			

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Article 12	Article 12	~~Article 12~~	
Union NIS cooperation plan	Union NIS cooperation plan	~~Union NIS cooperation plan~~	
Deleted with some provisions accommodated in articles 8a/8b			

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Article 13	*Article 13*	*Article 13*	*Article 13*
International cooperation	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.	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.*** (AM 94)	~~Without prejudice to the possibility for the cooperation network to have informal international cooperation,~~ The Union may conclude international agreements **in accordance with Article 218 TFEU** 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 **sensitive data, including** ~~the~~ personal data circulating **within** ~~on~~ the cooperation **group** ~~network~~.	(no change since March)

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	Article 13 a (new)		
	Level of criticality of market operators		
	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. (AM 95)		

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
CHAPTER IV SECURITY OF THE NETWORKS AND INFORMATION SYSTEMS OF PUBLIC ADMINISTRATIONS AND MARKET OPERATORS			**CHAPTER IV** **SECURITY OF THE NETWORKS AND INFORMATION SYSTEMS OF OPERATORS OF ESSENTIAL SERVICES**[28]
Article 14	*Article 14*	*Article 14*	*Article 14*
Security requirements and incident notification	Security requirements and incident notification	Security requirements and incident notification	Security requirements and incident notification

[28] Following recital to be provided with regard to public administrations not covered in Annex II:
(x) This directive does not apply to public administrations other than those <u>entities referred to in Annex II and</u> identified as operators of essential services. It is the responsibility of Member States to ensure the security of network and information systems of public administrations not falling within the scope of this Directive.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
1. Member States shall ensure that public administrations and market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.	1. Member States shall ensure that ~~public administrations and~~ 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, ~~these~~ ***those*** measures shall ~~guarantee~~ ***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 ~~system~~ ***systems*** on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems. (AM 96)	1. Member States shall ensure that ~~market~~ operators **of essential services** ~~and public administrations~~ take appropriate **and proportionate** technical and organisational measures to manage the risks posed to the security of ~~the~~ network**s** and information systems which they control and use in their operations. Having regard to the state of the art, **those** measures shall **ensure** ~~guarantee~~ a level of security **of networks and information systems** appropriate to the risk presented.	1. Member States shall ensure that ~~market~~ operators **of essential services** ~~and public administrations~~ take appropriate **and proportionate** technical and organisational measures to manage the risks posed to the security of ~~the~~ network**s** and information systems which they ~~control and~~ use in their operations. Having regard to the state of the art, **those** measures shall **ensure** ~~guarantee~~ a level of security **of networks and information systems** appropriate to the risk presented.[29]

[29] To be accompanied by the following recital:

(x) **Measures to manage the risk include measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact; the security of network and information systems comprises the security of stored, transmitted and processed data; the analysis of this data is part of the identification of the risks.**

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		1a ~~In particular,~~ **Member States shall ensure that operators of essential services take appropriate** measures ~~shall be taken~~ to prevent and minimise the impact of incidents affecting ~~their~~ **security of the** network**s** and information systems ~~on~~ **used for the provision of** ~~the~~ **essential** ~~core~~ services ~~they provide~~ and thus **to** ensure the continuity of **those** ~~the~~ services ~~underpinned by those networks and information systems~~.	**1a Member States shall ensure that operators of essential services take appropriate** measures to prevent and minimise the impact of incidents affecting **security of the** network**s** and information systems **used for the provision of essential** services and thus ~~**to ensure**~~ **striving to maintain** the continuity of **those** services.
2. Member States shall ensure that public administrations and market operators notify to the competent authority incidents having a significant impact on the security of the core services they provide.	2. Member States shall ensure that ~~public administrations and~~ market operators notify ***without undue delay*** to the competent authority ***or to the single point of contact*** incidents having a significant impact on the ~~security~~ ***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 public administrations and market~~ operators **of essential services shall** notify **without undue delay** to the competent authority **or to the CSIRT** incidents having a significant impact on ~~the security of~~ the **continuity** ~~security~~ of the **essential** ~~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 require**~~ **ensure** ~~that public administrations and market~~ **that** operators **of essential services** ~~**shall to**~~ notify **without undue delay** to the competent authority **or to the CSIRT** incidents having a significant impact on ~~the security of~~ the **continuity** ~~security~~ of the **essential** ~~core~~ services they provide**. Notifications shall include relevant information allowing the competent authority or CSIRT to determine the cross-border effect of the incident. Notification shall not expose the notifying party to increased liability.**

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	To determine the significance of the impact of an incident, the following parameters shall inter alia be taken into account: (AM 97)	**2a To determine the significance of the impact of an incident, the following parameters in particular shall be taken into account**	(no change since March)
	(a) the number of users whose core service is affected; (AM 98)	**a) the number of users affected by the disruption of the essential service;**	
	(b) the duration of the incident; (AM 99)	**b) the duration of the incident;**	
	(c) geographic spread with regard to the area affected by the incident. (AM 100)	**(c) the geographical spread with regard to the area affected by the incident.**	
	Those parameters shall be further specified in accordance with point (ib) of Article 8(3). (AM 101)		

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	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. (AM 102)		

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		2ac When notifying an incident to its national competent authority or CSIRT, an operator of essential services shall include relevant information allowing the competent authority or CSIRT to determine the cross-border effect of that incident. Based on the information provided by the operator, the competent authority or CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. In doing so, the competent authority or CSIRT shall preserve the operator's security and commercial interests as well as the confidentiality of the information provided by the operator. **~~The operator shall be informed, as soon as possible, about any undertaken steps, results and any other information with relevance to the incident.~~** **At the request of the competent authority or CSIRTs, the single point of contact shall forward notifications referred to in the first subparagraph to single points of**	**2ac ~~When notifying an incident to its national competent authority or CSIRT, an operator of essential services shall include relevant information allowing the competent authority or CSIRT to determine the cross-border effect of that incident.~~ Based on the information provided by the operator of essential services, the notified competent authority or CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. In doing so, the competent authority or CSIRT shall, in accordance with Union law or national legislation that complies with Union law, preserve the operator's security and commercial interests as well as the confidentiality of the information provided by the operator.** **~~The operator shall be informed, as soon as possible, about any undertaken steps, results and any other information with relevance to the incident.~~** **Where the circumstances allow for it, the competent authority or CSIRT shall provide the notifying operator of essential services with relevant information with regards to the follow-up of the notification**

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		contact in other affected Member States.	**of an incident, such as information that could support the effective handling of the incident.** **At the request of the competent authority or CSIRTs, the single point of contact shall forward notifications referred to in the first subparagraph to single points of contact in other affected Member States.**
	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. (AM 103)		

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	2c. Market operators not covered by Annex II may report incidents as specified in Article 14(2) on a voluntary basis. ***(AM 104)***		**2c. Without prejudice to Article 2, ~~E~~entities ~~not covered by Annex II~~ which have not been identified as operators of essential services may ~~report~~ notify incidents having a significant impact on the continuity of the services they provide ~~as specified in Article 14(2)~~ on a voluntary basis.** **When processing notifications, Member States shall act in accordance with the procedure set out in ~~Article 14~~ this Article. Member States ~~shall be entitled to give~~ may process mandatory notifications in priority ~~over~~ to voluntary notifications. Voluntary notifications shall only be processed where ~~the competent authority or CSIRT considers that~~ such processing does not constitute a disproportionate or undue burden on ~~them~~ Member States. Voluntary notification shall not result in the imposition upon the notifying entity of any obligations to which it would not have been subject had it not given that notification.** [30]

[30] **To be accompanied by the following recital :**

Entities that have not been identified as operators of essential services and that would therefore fall outside the scope of this Directive, may be affected by incidents having a significant impact on the continuity of the services they provide. Those entities might consider that it is in the public interest to notify the relevant authorities of Member States of the occurrence of such incidents. In such circumstances entities may notify these incidents on a voluntary basis.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
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 **to** ~~and~~ 2**b** apply to ~~all~~ ~~market~~ **the following** operators **of essential services:** **- operators of essential services that are established in a Member State; and** **- operators of essential services that are not established in the Union but direct their activities to one or several Member States** ~~providing services within the European Union~~.	~~**3. The requirements under paragraphs 1 to 2b apply to the following operators of essential services:**~~ ~~**- operators of essential services that are established in a Member State; and**~~ ~~**- operators of essential services that are not established in the Union but direct their activities to one or several Member States.**~~

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
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.	4. ~~The~~ ***After consultation with the notified*** competent authority ***and the market operator concerned, the single point of contact*** may inform the public ~~, or require the public administrations and operators to do so, where it determines that~~ ***about individual incidents, where it determines that public awareness is necessary to prevent an incident or deal with an on-going 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.*** ~~of the incident is in the public interest~~	4. **After consulting the operator of essential services concerned,** ~~The~~ the **notified** competent authority **or CSIRT** may inform the public, or require the ~~market~~ operators **of essential services** ~~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~~.	(no change since March)

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	Before any public disclosure ~~***of the incident is in the public interest***~~***, 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.		
	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.		

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
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.	Once a year, the ~~competent authority~~ ***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. (AM 105)	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~~ **paragraphs 2 and 2ac** ~~paragraph~~.	~~**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 paragraphs 2 and 2ac paragraph.**~~
	4a. Member States shall encourage market operators to make public incidents involving their business in their financial reports on a voluntary basis. (AM 106)		

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
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.	~~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.~~ (AM 107)		
6. ***Subject to any delegated act adopted under paragraph 5, the competent authorities*** may adopt guidelines ***and, where necessary, issue instructions*** concerning the circumstances in which ***public administrations and*** market operators are required to notify incidents.	6. ~~Subject to any delegated act adopted under paragraph 5, the competent authorities~~ ***The competent authorities or the single points of contact*** may adopt guidelines ~~and, where necessary, issue instructions~~ concerning the circumstances in which ~~public administrations and~~ market operators are required to notify incidents. (AM 108)	6. ~~Subject to any delegated act adopted under paragraph 5, the competent authorities~~ **The competent authorities, when requested with the assistance of ENISA,** may adopt guidelines ~~and, where necessary, issue instructions~~ concerning the circumstances in which ~~public administrations and~~ ~~market~~ operators **of essential services** are required to notify incidents.	6. ~~Subject to any delegated act adopted under paragraph 5, the competent authorities~~ **The ~~competent authorities, when requested~~ Member States, after discussion in the cooperation group in accordance with point (n) of Article 8a(3) ~~with the assistance of ENISA when requested~~,** may adopt guidelines ~~and, where necessary, issue instructions~~ concerning the circumstances in which ~~public administrations and~~ ~~market~~ operators **of essential services** are required to notify incidents, **including on the parameters to determine the significance of the impact of an incident as referred to in paragraph 2a. <u>These guidelines shall take utmost account of the outcome of the discussions within the cooperation group.</u>**

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
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	(no change since March)
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[31].	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. (AM 109)	deleted	(no change since March)

31 OJ L 124, 20.5.2003, p. 36.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	8a. Member States may decide to apply this Article and Article 15 to public administrations mutatis mutandis. (AM 110)		

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Article 15	*Article 15*	*Article 15*	*Article 15*
Implementation and enforcement	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.	1. Member States shall ensure that the competent authorities ~~have all~~ ***and the single points of contact have*** the powers necessary to ~~investigate cases of non-compliance of public administrations or~~ ***ensure compliance*** of market operators with their obligations under Article 14 and the effects thereof on the security of networks and information systems. (AM 111)	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 **of essential services** ~~and~~ 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 **powers and means** to **assess** ~~investigate~~ **the** ~~cases of non-~~compliance of ~~public administrations or~~ ~~market~~ operators **of essential services** ~~and~~ with their obligations under Article 14 and the effects thereof on the security of networks and information systems.
2. Member States shall ensure that the competent authorities have the power to require market operators and public administrations to:	2. Member States shall ensure that the competent authorities ***and the single points of contact*** have the power to require market operators ~~and public administrations~~ to: (AM 112)	2. Member States shall ensure that the competent authorit**y**~~ies~~ has~~ve~~ the **means** ~~power~~ to require ~~market~~ operators ~~**of essential services** and public administrations~~ to:	2. Member States shall ensure that the competent authorit**y**~~ies~~ has~~ve~~ the **powers and means** ~~power~~ to require ~~market~~ operators ~~**of essential services** and public administrations~~ to:

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
(a) provide information needed to assess the security of their networks and information systems, including documented security policies;		(a) provide information needed to assess the security of their networks and information systems, including documented security policies;	
(b) undergo a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority.	(b) ~~undergo~~ ***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 ~~results thereof~~ ***evidence*** available to the competent authority ***or to the single point of contact***. (AM 113)	(b) ~~undergo a security audit carried out by a qualified independent body or national authority~~ **provide evidence of effective implementation of security policies, such as the results of a security audit carried out by the competent authority or a qualified ~~external or internal~~ auditor** and**, in the latter case,** make the results thereof available to the competent authority.	(b) ~~undergo a security audit carried out by a qualified independent body or national authority~~ **provide evidence of effective implementation of security policies, such as the results of a security audit carried out by the competent authority or a qualified ~~external or internal~~ auditor** and**, in the latter case,** make the results thereof**, including the underlying evidence,** available to the competent authority.
	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. (AM 114)		**When sending that request, the competent authorities shall state the purpose of the request and ~~sufficiently~~ specify what information is required.**

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
3. Member States shall ensure that competent authorities have the power to issue binding instructions to market operators and public administrations.	3. Member States shall ensure that ***the*** competent authorities ***and the single points of contact*** have the power to issue binding instructions to market operators ~~and public administrations~~.	3. ~~Member States shall ensure that~~ **Following the assessment of information or results of security audits referred to in paragraph 2,** the competent authorit**y**~~ies have the power to~~ **may issue** binding instructions to the ~~market~~ operators ~~and public administrations~~ **of essential services to remedy their operations.**	(no change since March)
	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:		

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	(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	EP	COUNCIL	PRESIDENCY PROPOSALS
	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. (AM 116)		
4. The competent authorities shall notify incidents of a suspected serious criminal nature to law enforcement authorities.	4. The competent authorities ~~shall notify incidents of a suspected serious~~ criminal ~~nature to~~ ***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. (AM 117)	deleted	(no change since March)

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
5. The competent authorities shall work in close cooperation with personal data protection authorities when addressing incidents resulting in personal data breaches.	5. ***Without prejudice to applicable data protection 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.*** (AM 118)	5. The competent authorit~~yies~~ shall work in close cooperation with personal data protection authorities when addressing incidents resulting in personal data breaches.	(no change since March)
6. Member States shall ensure that any obligations imposed on public administrations and market operators under this Chapter may be subject to judicial review.	6. Member States shall ensure that any obligations imposed on ~~public administrations and~~ market operators under this Chapter may be subject to judicial review. (AM 119)	deleted	(no change since March)
	6a. Member States may decide to apply Article 14 and this Article to public administrations mutatis mutandis. (AM 120)		

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			Article 15aa
			Jurisdiction and territoriality
			~~**1. For the purposes of this Directive, an operator of essential services shall be deemed to be under the jurisdiction of a Member State where it has been identified as provides providing an essential service in the territory of that Member State.**~~
			~~**2. If an operator of essential services has been identified as provides providing essential services in more than one Member State, it shall be deemed to be under the separate and concurrent jurisdiction of each of these Member States.**~~

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			Chapter IVa **SECURITY OF NETWORKS AND INFORMATION SYSTEMS OF DIGITAL SERVICE PROVIDERS**[32]

[32] (x) Many EU businesses rely on Digital Service Providers (DSPs) as defined in this Directive for the provision of their own services. **As some digital services can be an important resource for their users, including operators of essential services, and as such users may not always have alternatives available, this Directive should also apply to providers of such services.** The security, continuity and reliability of the type of services referred to in Annex III is of the essence for the smooth functioning of **~~those~~ many** businesses~~,~~**. A disruption of a digital service as listed in Annex III could prevent the provision of other services which rely on it and could thus have an impact on key economic and societal activities in the Union. Such digital services ~~are~~ may therefore be of ~~essential~~ crucial importance for the smooth functioning of businesses that depend on them** and **moreover** for ~~their~~ **the** participation **of such businesses** in the internal market and cross-border trade across the Union. The DSPs included in this Directive are those considered to offer digital services on which many EU businesses ~~do~~ increasingly rely. **DSPs are defined in this Directive for the sole purpose of this Directive.**

(x) Given the fundamental differences between operators of essential services**, (**in particular their direct link with physical infrastructure**)** and DSPs**, (**in particular their cross-border nature**)**, this Directive ~~under~~takes a different approach in relation to each of those groups of actors. The approach for DSPs aims at creating a higher level of harmonisation for such providers which are usually active in many Member States. This allows them to be treated in a similar way across the EU, in a manner proportionate to their nature and degree of risk they may pose. As part of this approach, this Directive should apply to all DSPs meeting the definitions, thus ensuring its uniform application across the Union.

~~(x) As some digital services can be an essential resource for their users and may not always have alternatives available, including operators providing essential services for the maintenance of critical societal and economic activities, this Directive should also apply to those services. Digital services should be considered as essential resources when a significant number of other digital services or other services rely on a digital service as a key input. Disruption of such essential resources would prevent the provision of its dependent digital services and would thus have an impact on key economic and societal activities in the Union. They are therefore essential for the smooth functioning of their dependent businesses and moreover for their participation in the internal market and cross-border trade across the Union.~~

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			Article 15a
			~~Digital servic providers~~ Security requirements and incident notification
			1. Member States shall ~~require~~ ensure that digital service providers ~~to~~ identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems which they ~~control and or~~ use ~~in their operations~~ in the context of offering services as referred to in Annex III within the Union. Having regard to the state of art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.[33]

[33] (x) DSPs should ensure a level of security commensurate to the degree of risk posed to the security of the services they provide, given the importance of their services to the operations of other businesses within the EU. In practice the degree of risk for operators of essential services, which are often essential for the maintenance of critical societal and economic activities, will be higher than for DSPs. Therefore the security requirements for DSPs should be lighter. DSPs should remain free to take measures they consider appropriate to manage the risks posed to the security of their networks and information systems. **Because of their cross-border nature, DSPs should be subject to a more harmonised**

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			1a. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting the security of the digital service provider's networks and information systems on the services as referred to in Annex III **that are offered within the Union**, **thus** ~~**ensuring**~~ **striving to maintain the continuity of those services.**

approach at the European level~~. In addition~~,**. In particular DSPs could take into account ENISA guidelines when elaborating their security measures.** ~~Implementing acts could facilitate the specification and implementation of such measures.~~

(x)There may be situations where operators of essential services rely on the service of a digital service provider, for example a cloud service, for the provision of an essential service. In such a case the operator of essential services should ensure that the cloud computing service provider, having regard to the state of the art, implements technical and organisational security measures which are appropriate and proportionate to the risk presented and help protect the network and information systems of the operator of essential services.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			2. Member States shall ~~require~~ ensure that digital service providers notify any ~~substantial~~ incident having a substantial impact on the provision of a service[34] ~~with regard to the services~~ as referred to in Annex III to the competent authority or to the CSIRT without undue delay ~~after having become aware of it~~. Notifications shall include information to enable the competent authority or CSIRT to determine the significance of any cross-border impact. Notification shall not expose the notifying party to increased liability.

[34] **~~To be accompanied by the following recital:~~**
~~(x) DSPs should notify to the competent authority or CSIRT only those incidents that have a substantial impact on the service provided. An incident should be considered as substantial where the disruption of the service provided by the DSP is such that its dependent services cannot properly function for a significant period of time.~~

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			2a. An incident shall be considered as having a substantial impact on the provision of the service where the following criteria are fulfilled: **a) the functioning of the service is seriously disrupted;** **b) a high number of users are affected by the disruption of the service, in particular users relying on the service for the provision of their own services ;** **c) the duration of the incident is significant;** **(d) the impact on economic and societal activities is profound.** **The obligation to notify an incident shall only apply where the DSP has access to the information required to appreciate if the criteria are fulfilled.**

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			2b. Where an operator of essential services relies on a third-party cloud computing service to provide a service which is essential for the maintenance of critical societal and economic activities, the contract may include a requirement that the cloud computing service provider notifies incidents solely to the operator of essential services. In such a case, Article 14(2) shall apply and the digital service provider shall not be obliged to notify the incident in addition to the competent authority or CSIRT.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			3. Where appropriate, in particular if the incident referred to in paragraph 2 concerns two or more Member States, the notified competent authority or the CSIRT shall inform other affected Member States. In doing so, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the digital service provider's security and commercial interests as well as the confidentiality of the information provided.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			3a. After consulting the digital service provider concerned, the notified competent authority or CSIRT, and, where appropriate, the authorities or CSIRTS of other Member States concerned may inform the public or require the digital service provider to do so, where it determines that disclosure of the incident is in the public interest.
			4. ENISA shall ~~adopt~~ publish guidelines concerning the measures referred to in paragraph 1 and the notifications referred to in paragraph 2. **~~If necessary, after consulting ENISA, the Commission may, by means of implementing acts, further specify:~~** **~~- the measures referred to in paragraph 1;~~** **~~- the details on notification as referred to in paragraph 2, taking into account that the notification procedure shall not create unreasonable burden for digital service providers.~~** **~~Those implementing acts shall be adopted in accordance with the examination procedure referred to in article19(3).~~**

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			5. This article shall not apply to micro- and small enterprises as defined in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises[35]

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

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			Article 15b
			Implementation and enforcement
			1. Member States shall ensure that the competent authorities take action, if necessary, through ex post supervisory activities, when ~~informed~~ provided with evidence that a digital service provider ~~allegedly~~ does not meet the requirements laid down in Article 15a. Such evidence may also be submitted by a competent authority of another Member State where the service is provided.[36]
			2. For the purpose of paragraph 1, the competent authorities shall have the necessary powers and means to: **(a) require digital service providers to provide information needed to assess the security of their networks and information systems including documented security policies** **(b) require that digital service providers**

[36] (x) DSPs should be subject to light-touch and reactive ex post supervisory activities justified by the nature of their services and operations. The competent authority should therefore only take action when ~~it is~~ ~~informed~~ **provided with evidence** (**inter alia** by the DSP **itself**, by another competent authority**, including a competent authority of another Member State,** or by a user **of the service**) that a DSP ~~might~~ **does** not comply with the requirements of this Directive**, in particular ~~with regards to~~ following an incident that has occurred**. The competent authority should therefore have no general obligation to supervise DSPs.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			remedy any failure to fulfil the requirements laid down in article 15a.
			3. If a digital service provider has its main establishment or a representative in one Member State, but its networks and information systems are located in one or more other Member States, the competent authority of the Member State of the main establishment or of the representative and the competent authorities of these other Member States shall cooperate and assist each other as necessary. Such assistance and cooperation may cover information exchanges between competent authorities concerned and requests to carry out the supervisory measures referred to in ~~Article 15b~~ paragraph 2.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			Article 15c
			Jurisdiction and territoriality[37]
			1. For the purposes of this Directive, a digital service provider shall be deemed to be under the jurisdiction of the Member State where it has its main establishment. A digital service provider shall be deemed to have its main establishment in a Member State when it has its head office in the Union in that Member State.

[37] To be accompanied by the following recital:

(x) Jurisdiction for digital service providers should be attributed to only one Member State, where the operator has its main establishment in the Union, which in principle corresponds to the place where the provider has its head office **in the Union** and where the main decisions concerning network and information security are taken. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect. This criterion should not depend on whether the network and information systems are physically located in that place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not criteria for determining the main establishment.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			2. A digital service provider that is not established in the Union, but ~~provides~~ offers services as referred to in Annex III within the Union, shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. The digital service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established. [38]

[38] To be accompanied by the following recital:

(x) Where a digital service provider not established in the Union **~~provides its services in one or more Member States~~offers services within the Union**, it should designate a representative. The representative should act on behalf of the digital service provider and competent authorities or CSIRTs may contact the representative. The representative should be explicitly designated by a written mandate of the digital service provider to act on his behalf with regard to the latter obligations, including incident reporting, under this Directive.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			~~**3. If a digital service provider has its main establishment or a representative in one Member State, but its networks and information systems are located in one or more other Member States, the competent authority of the Member State of the main establishment or of the representative and the competent authorities of these other Member States shall cooperate and assist each other as necessary. Such assistance and cooperation may cover information exchanges between competent authorities concerned and requests to carry out the supervisory measures referred to in Article 15b.**~~

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			4. The designation of a representative by the ~~operator~~ digital service provider shall be without prejudice to legal actions which could be initiated against the ~~operator~~ digital service provider itself.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			CHAPTER IVb
			STANDARDISATION
Article 16	*Article 16*	*Article 16*	*Article 16*
Standardisation	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.	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. (AM 121)	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 **European or internationally accepted** standards and/or specifications relevant to networks and information security.	1. To promote convergent implementation of Article 14(1)~~, and~~ 14(1a)**, ~~and~~ 15a(1) and 15a(1a)** Member States shall, without **~~prejudice to technological neutrality~~ imposing or discriminating in favour of the use of a particular type of technology**, encourage the use of European or internationally accepted standards and/or specifications relevant to networks and information security.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		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.	**1a. The European Network and Information Security Agency ("ENISA"), in collaboration with Member States, ~~may~~ shall elaborate ~~recommendations~~ advice 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.**
2. The Commission shall draw up, by means of implementing acts a list of the standards referred to in paragraph 1**.** The list shall be published in the Official Journal of the European Union.	2. The Commission shall ***give a mandate to a relevant European standardisation body to***, ***in consultation with relevant stakeholders,*** draw up~~, by means of implementing acts~~ 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. (AM 122)	deleted	**~~2. Taking into account the ENISA advice and guidelines referred to in paragraph 1a, and in accordance with Regulation (EU) 1025/2012 of the European Parliament and the Council the Commission may draw up, by means of implementing acts a list of the standards and specifications referred to in paragraph 1. The list shall be published in the Official Journal of the European Union. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).~~**

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
CHAPTER V FINAL PROVISIONS			CHAPTER V FINAL PROVISIONS
Article 17	*Article 17*	*Article 17*	*Article 17*
Sanctions	*Sanctions*	*Sanctions*	~~*Sanctions*~~*Penalties*
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 **Articles 14 and 15 of** this Directive and shall take all measures necessary to ensure that they are implemented. The sanctions provided for must be effective, proportionate and dissuasive. ~~The Member States shall notify those provisions to the Commission by the date of transposition of this Directive at the latest and shall notify it without delay of any subsequent amendment affecting them.~~	1. Member States shall lay down **the** rules on ~~**sanctions**~~**penalties** applicable to infringements of the national provisions adopted pursuant to ~~**Articles 14, and 15, and 15a and 15b of**~~ this Directive and shall take all measures necessary to ensure that they are implemented. The ~~**sanctions**~~**penalties** provided for ~~**musts**~~**shall** be effective, proportionate and dissuasive. **Member States shall notify [by the date of transposition of this Directive] the Commission of those rules and of those measures and shall notify it without delay of any subsequent amendment affecting them.**

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	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. (AM 123)		
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[39].		deleted	

[39] SEC(2012) 72 final

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Article 18	Article 18	~~Article 18~~	
Exercise of the delegation	Exercise of the delegation	~~Exercise of the delegation~~	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Article 19	*Article 19*	*Article 19*	*Article 19*
Committee procedure	Committee procedure	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.	(no change since March)
2. Where reference is made to this paragraph, Article 4 of Regulation (EU) No 182/2011 shall apply.		deleted	(no change since March)
3. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.		3. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	(no change since March)

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Article 20	*Article 20*	*Article 20*	*Article 20*
Review	Review	Review	Review
			~~1. By (…) (1 year after the transposition), the Commission shall assess whether the approach taken by Member States in the identification of the operators of essential services is consistent and report to the Cooperation Group.~~ **1. The Commission shall submit a ~~transposition~~ report to the European Parliament and to Council by [~~18 months~~ 1 year after the date of transposition], ~~including in particular an assessment of~~ assesing the consistency of the approach taken by Member States in the identification of the operators of essential services.**

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
The Commission shall periodically review the functioning of this Directive and report to the European Parliament and the Council. The first report shall be submitted no later than three years after the date of transposition referred to in Article 21. For this purpose, the Commission may request Member States to provide information without undue delay.	The Commission shall 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. (AM 126)	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** ~~three~~ years after the date ~~of transposition~~ referred to in Article 21(2). **Thereafter, the Commission shall periodically review this Directive.** 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.** ~~may request Member States to provide information without undue delay~~.	**2.** The Commission shall periodically review the functioning of this Directive**~~, in particular the lists contained in Annex II and Annex III~~**, and report to the European Parliament and to the Council. **~~The first report shall be submitted no later than three years after the date referred to in Article 21(2).~~** ~~Thereafter, the Commission shall periodically review this Directive.~~ **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.** In its review the Commission shall also assess **the list contained in Annex II and III, and** the consistency in the identification of operators **of essential services** and services in the sectors referred to in Annex II. **The first report shall be submitted no later than three years after the date referred to in Article 21(~~2~~1).**

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
		Article 20a	*Article 20a*
		Transitional measures	Transitional measures
		1. Without prejudice to Article 21 and with a view of providing Member States with additional possibilities for appropriate cooperation during the period of transposition, the Cooperation Group and the CSIRTs Network shall begin to perform their tasks set out respectively in Articles 8a(3) and 8b(3) by (6 months after the date of entry into force of this Directive).	(no change since March)

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			1a. **~~By (date of transposition 6 months after entry into force~~**), ~~and~~ **In the period between the dates set out in paragraph 1 and in article 21(1)**, for the purposes of supporting Member States **to take a consistent approach** in the process ~~related to the~~ **of** identification of operators **of essential services**, the Cooperation Group shall **~~be responsible for~~** discuss~~ing~~**~~, at the request of the Member State~~, the process, substance and the type of** national measures **and, at the request of a Member State, draft national measures of that Member State, ~~of that requesting Member States~~** allowing for the identification of operators **of essential services within a specific sector in accordance with the criteria set out in Articles 3a and 3b.**
		2. By (the date referred to in Article 21(2)) and for the purposes of this Article, Member States shall ensure appropriate representation in the Cooperation Group and the CSIRTs Network.	**2. By (~~the date referred to in Article 21(2)~~ 6 months after entry into force) and for the purposes of this Article, Member States shall ensure appropriate representation in the Cooperation Group and the CSIRTs Network.**

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Article 21	*Article 21*	*Article 21*	*Article 21*
Transposition	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.	(no change since March)
They shall apply those measures from [one year and a half after adoption].		**2**. They shall apply those measures from **two years** ~~one year~~ and a half after ~~adoption~~ the ~~-~~**date of entry into force of this Directive.**	~~**2. They shall apply those measures from two years one year and a half after adoption the date of entry into force of this Directive.**~~
			~~**2a. Member State shall carry out an initial identification of operators of essential services in accordance with Article 3a by two and a half years after the date of entry into force of this Directive.**~~

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
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.	
			2a. Member State shall carry out an initial identification of operators of essential services in accordance with Article 3a by two and a half years after the date of entry into force of this Directive.
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.		deleted	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Article 22	*Article 22*	*Article 22*	*Article 22*
Entry into force	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.*	(no change since March)

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
Article 23	*Article 23*	*Article 23*	*Article 23*
Addressees	Addressees	Addressees	Addressees
This Directive is addressed to the Member States.	This Directive is addressed to the Member States.,	This Directive is addressed to the Member States.	
Done at Brussels	Done at Brussels	Done at Brussels	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
ANNEX I	ANNEX I	ANNEX I	ANNEX I
Requirements and tasks of the Computer Emergency Response Team (CERT)	Requirements and tasks of the Computer Emergency Response ~~Team~~ ***Teams (CERTs)*** (AM 127)	Requirements and tasks of the Computer **Security Incident** ~~Emergency~~ **Response** Team **(CSIRT)** ~~(CERT)~~	(no change since March)
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.	(a) The ~~CERT~~ ***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. (AM 128)	(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.	(a) The CSIRT 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.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
(b) The CERT shall implement and manage security measures to ensure the confidentiality, integrity, availability and authenticity of information it receives and treats.		deleted	
(c) The offices of the CERT and the supporting information systems shall be located in secure sites**.**	(c) The offices of the ~~CERT~~ ***CERTs*** and the supporting information systems shall be located in secure sites ***with secured network information systems.*** (AM 129)	(c) The offices of the **CSIRT** ~~CERT~~ and the supporting information systems shall be located in secure sites.	
(d) A service management quality system shall be created to follow-up on the performance of the CERT and ensure a steady process of improvement. It shall be based on clearly defined metrics that include formal service levels and key performance indicators.		deleted	
(e) Business continuity:		(e) Business continuity:	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
- 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 **available** ~~set up for the CERT to ensure permanent access to the means of communication~~.	
			(f) The CSIRT shall have the possibility to participate, where appropriate, in international cooperation networks.
(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,	- ***Detecting and*** monitoring incidents at a national level, (AM 130)	- Monitoring incidents at a national level,	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
- 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,	
- 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,		deleted	
	- Actively participating in Union and international CERT cooperation networks (AM 131)	**- Participating in the CSIRTs network.**	
- Organising campaigns on NIS;		deleted	
(b) The CERT shall establish cooperative relationships with private sector.		(b) The **CSIRT** ~~CERT~~ shall establish cooperative relationships with private sector.	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
(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,		deleted	
- information exchange formats on risks, incidents, and system naming conventions.		deleted	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
ANNEX II	ANNEX II	ANNEX II	
List of market operators	List of market operators	**List of types of entities for the purposes of Article 3(8) operators**	See Annex II in a separate table
Referred to in Article 3(8) a):	~~Referred to in Article 3(8) a):~~	**0. In the field of digital infrastructure**:	
		Internet exchange points	
		national domain name registries, domain name system service providers	
Referred to in Article 3(8) b):		**01 In the field of digital service platforms:**	
1. e-commerce platforms	~~1. e-commerce platforms~~	**(a)** e-commerce platforms	
2. Internet payment gateways	~~2. Internet payment gateways~~	**(b)** Internet payment gateways	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
3. Social networks	~~3. Social networks~~	**(c)** Social networks	
4. Search engines	~~4. Search engines~~	**(d)** Search engines	
5. Cloud computing services	~~5. Cloud computing services~~	**(e)** Cloud computing services	
6. Application stores	~~6. Application stores~~	**(f)** Application stores	
Referred to in Article (3(8) b):	~~Referred to in Article (3(8) b):~~ (AM 132)		
List of market operators	List of market operators		
1. Energy	1. Energy	**1. Energy**	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	(a) Electricity	***(a) Electricity***	
- Electricity and gas suppliers	~~– Electricity and gas -~~ Suppliers	**- Suppliers**	
- Electricity and/or gas distribution system operators and retailers for final consumers	~~- Electricity and/or gas~~ - Distribution system operators and retailers for final consumers	**- Distribution system operators**	
- Natural gas transmission system operators, storage operators and LNG operators	~~- 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	***(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	**- Operators of oil production, refining and treatment facilities, storage and transmission**	
	(c) Gas	***(c) Gas***	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
- Electricity and gas market operators	- ~~Electricity and gas market operators~~ ***Suppliers***	**- Suppliers**	
	- Distribution system operators and retailers for final consumers	**- Distribution system operators**	
	- Natural gas transmission system operators, storage system operators and LNG system operators	**- 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 ~~oil~~ natural gas production, refining, ~~and~~ treatment facilities, ***storage*** facilities ***and transmission***	**- Operators of natural gas production, refining, treatment facilities, *storage* facilities *and transmission***	
	- Gas market operators (AM 133)	**- Gas market operators**	
2. Transport	2. Transport	**2. Transport**	
		(a) Air transport	
- Air carriers (freight and passenger air transport)	~~- Air carriers (freight and passenger air transport)~~	**- Air carriers (freight and passenger air transport)**	
		- Airports	
		- Traffic management control operators	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
- Maritime carriers (sea and coastal passenger water transport companies and sea and coastal freight water transport companies)	~~- Maritime carriers (sea and coastal passenger water transport companies and sea and coastal freight water transport companies)~~ ***(i) Traffic management control operators***	***(b) Rail transport***	
- Railways (infrastructure managers, integrated companies and railway transport operators)	~~- Railways (infrastructure managers, integrated companies and railway transport operators)~~ ***(ii) Auxiliary logistics services:***	**- Railways (infrastructure managers, integrated companies and railway transport operators)**	
- Airports	~~- Airports~~ ***- warehousing and storage,***	**- Traffic management control operators**	
- Ports	~~- Ports~~ ***- cargo handling, and***	***(c) Maritime transport***	
- Traffic management control operators	~~- Traffic management control operators~~ ***- other transportation support activities***	**(i) Maritime carriers (inland, sea and coastal passenger water transport companies and inland, sea and coastal freight water transport companies)**	
- Auxiliary logistics services (a) warehousing and storage, b) cargo handling and c) other transportation support activities)	~~- Auxiliary logistics services (a) warehousing and storage, b) cargo handling and c) other transportation support activities)~~ ***(b) Rail transport***		

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	(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		

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
	(iii) Traffic management control operators		
	(iv) Auxiliary logistics services:		
	- warehousing,		
	- cargo handling, and		
	- other transportation support activities		
	(d) Maritime transport		
	(i) Maritime carriers (inland, sea and coastal passenger water transport companies and inland, sea and coastal freight water transport companies) (AM 134)		
3. Banking: credit institutions in accordance with Article 4.1 of Directive 2006/48/CE.		3. Banking: credit institutions in accordance with Article 4.1 of Directive 2006/48/CE.	

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
4. Financial market infrastructures: stock exchanges and central counterparty clearing houses	4. Financial market infrastructures: ***regulated markets, multilateral trading facilities, organised trading facilities*** ~~stock exchanges~~ and central counterparty clearing houses (AM 135)	4. Financial market infrastructures: stock exchanges and central counterparty clearing houses.	
5. Health sector: health care settings (including hospitals and private clinics) and other entities involved in health care provisions		5. Health sector: healthcare ~~settings~~ **providers** (including hospitals ~~and private clinics~~) ~~and other entities involved in health care provisons~~ **as defined in Article 3(g) of Directive 2011/24/EU**.	
	5a. Water production and supply (AM 136)	**6. Drinking water production and supply sector.**	
	5b. Food supply chain (AM 137)		
	5c. Internet exchange points(AM 138)		

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			ANNEX III
			Types of digital services ~~providers~~ for purposes of Article 3(8)(a)new
			For the purpose of this Directive, the following definitions shall apply

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			1. Online/e-commerce marketplace[40] An online marketplace is a digital service that allows **~~users~~** **consumers and/or traders, as defined respectively in Article 4(1)(a) and 4(1)(b) of Directive 2013/11/EU**, to conclude online sales and service contracts with **~~third parties~~** **traders**, **~~whether integrated~~** **either** on the online marketplace's website or on a **~~customised~~** **~~seller~~** **trader**'s website **that uses computing services provided by the online marketplace** **~~, by means of remote computing services, such as processing of transactions, aggregations of data or profiling of users,~~**.

[40] To be accompanied by a following recitals:
(x) An e-commerce platform/online marketplace is to be understood as a service which enables online sales with third parties. In this respect, application stores, which operate as online stores enabling the digital distribution of applications or software programmes is to be understood as being a type of e-commerce platform/online marketplace.
An online marketplace should allow consumers and/or traders to conclude online sales and service contracts with traders, and should be the final destination for the conclusion of those contracts. It should not cover online services that serve only as an intermediary to third-party services where a contract can ultimately be concluded. It should therefore not cover online services that compare the price of particular products or services from different traders, and then redirect the user to the preferred trader to purchase the product. Computing services provided by the online marketplace may include processing of transactions, aggregations of data or profiling of users.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			2. Social network 'A social network' is a digital service **dedicated to** enable users to exchange ~~information and content and interact~~**,** via a**n** ~~dedicated~~ individual**ised** profile created on the service**, information or content with other users and generate a list of users with whom they are connected**.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			3. Online search engine[41] 'An online search engine' is a digital service that allows users to perform searches **~~on the~~ of in principle all websites ~~of third parties~~ or a geographical subset thereof,** on the basis of a a **query on any subject in the form of a** keyword, phrase or other input **~~specified by the user in a query. It~~ and** returns ~~a list of~~ links in which information related to the requested content can be found.

[41] **To be accompanied by the following recital:**
(x) An online search engine should allow the user to perform searches of in principle all websites on the basis of a query on any subject. The scope of the search may be limited to a specific geographical area. The definition of an online search engine provided in this Directive should not cover search functions that are limited to the content of a specific website, irrespective of whether the search function is provided by an external search engine. It should also not cover online services that compare the price of particular products or services from different traders, <u>and then redirect the user to the preferred trader to purchase the product</u>.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			4. Cloud computing service 'A Cloud Computing service is a digital service that **~~provides a~~** **enables** **access to** scalable and elastic pool of shareable **~~physical and virtual~~** computing resources **~~with self-service provisioning and administration on-demand through network access, using a defined interface~~**.[42]

[42] To be accompanied by the following recital:
Cloud computing services span a wide range of activities that can be delivered according to different models. In order to distinguish cloud computing services from other information society services, to which digital services refer, the key characteristics of cloud computing services that are considered for this Directive are that these services enable access to a scalable and elastic pool of shareable computing resources. "Scalable", "elastic pool" and "shareable computing resources" mean, respectively, that these services, in order to handle fluctuations in demand, are flexibly allocated computing resources by the cloud service provider irrespective of the geographical location of the resources; that these services, in order to rapidly increase and decrease the maximum amount of work, are provisioned and released according to demand; and that these services are provided to multiple users who share a common access to the service, where the use of a service is separated for each user, although the service is provided from the same electronic equipment.

COMMISSION	EP	COUNCIL	PRESIDENCY PROPOSALS
			~~**5. Internet payment gateway**~~ ~~'An internet payment gateway' is a digital service that processes, verifies, authorises or declines online payments by automating the payment transaction between two parties on behalf of the merchant service.~~

ANNEX II

Sector	**Subsector**	**Type of entity for the purposes of Article 3(8)**
1. Energy	*a) Electricity*	- Electricity undertaking as defined in Article 2(35) of Directive 2009/72/EC, which carries out the function of "supply" as defined in Article 2(19) of Directive 2009/72/EC
		- Distribution system operators as defined in Article 2(6) of Directive 2009/72/EC
		- Transmission system operators as defined in Article 2(4) of Directive 2009/72/EC
	b) Oil	- Operator of **o**il transmission pipelines
		- Operators of oil production, refining and treatment facilities**, storage and transmission**
	c) Gas	- Supply undertakings as defined in Article 2(8) of Directive 2009/73/EC
		- Distribution system operators as defined in Article 2(6) of Directive 2009/73/EC
		- Transmission system operators as defined in Article 2(4) of Directive 2009/73/EC
		- Storage system operators as defined in Article 2(10) of Directive 2009/73/EC
		- LNG system operator as defined in Article 2(12) o Directive 2009/73/EC
		- Natural gas undertaking as defined in Article 2(1) of Directive 2009/73/EC

		- Operator of natural gas refining and treatment facilities
2. Transport	*(a) Air transport*	- Air carriers as defined in Article 3(4) of Regulation 300/2008
		- **Airport managing bodies as defined in Article 2(2) of Directive 2009/12/EC managing ~~A~~a**irports as defined in Article 2(1) of Directive 2009/12/EC, including the core airports listed in section 2 of Annex II of Regulation 1315/2013; **and entities operating ancillary installations contained within airports.**
		- Traffic management control operators providing air traffic control (ATC) service as defined in Article 2(1) of Regulation 549/2004
	(b) Rail transport	- Infrastructure managers as defined in Article **~~3(b) of Directive 2004/49/EC~~ 3(2) of Directive 2012/34/EU**
		- Railway undertakings as defined in **Article ~~3(c) of Directive 2004/49/EC~~ 3(1) of Directive 2012/34/EU, including operators of service facilities as defined in Article 3(12) of Directive 2012/34/EU**
	(c) ~~Maritime~~ Water transport	(i) inland, sea and coastal passenger and freight water transport companies, **as defined for maritime transport in Annex I of Regulation 725/2004/EC,** not including the individual vessels operated by those companies [43]

[43] To be accompanied by the following recitals:

		(ii) **Managing bodies of ~~P~~p**ort**s** as defined in Article 3(1) of Directive 2005/65/EC**, including their port facilities as defined in Article 2(11) of Regulation (EC) 725/2004; and entities operating works and equipment contained within ports**
		(iii) ~~traffic management control operators~~ **Operators of vessel traffic services, as defined in Article 3(o) of Directive 2002/59/EC**
	(d) Road Transport	**(i) Road authorities as defined in Article 2(12) of Commission Delegated Regulation (EU) 2015/962 responsible for ~~T~~traffic management control ~~operators~~**
		~~(ii) Operators of Intelligent Transport Systems as defined in Article 4(1) of Directive 2010/40/EU~~
3. Banking		- credit institutions as defined in Article 4 of Regulation 575/2013

(x) When identifying operators in the maritime sector, Member States should take into account existing and future international codes and guidelines developed in particular by the International Maritime Organisation, with a view to providing individual maritime operators with a coherent approach.

(x) **Security requirements for companies, ships, port facilities, ports and vessel traffic systems, under Union legal acts cover all operations including the radio and telecommunication systems, computer systems and networks. Part of the mandatory procedures to be followed includes the reporting of all security incidents and should therefore be considered as lex specialis ~~in the context of Article 1(7) of the present Directive, concerning explicit obligations on the security of networks and information systems or the notification of incidents in sector-specific Union legal acts~~**

4. Financial market infrastructures[44]		- **Operators of T**~~t~~rading venues as defined in Article 4 of Directive 2014/65/EU
		- Central counterparty as defined in Article 2 of

[44] To be accompanied by the following recitals:

(x) Regulation and supervision in the financial sector is highly harmonised at EU level, through the use of primary and secondary EU legislation, as well as technical standards developed together with the European Supervisory Authorities, which together form the Single European Rulebook for financial services. The application and supervision of this single rulebook to supervised entities and groups in the Banking Union is assured by the Single Supervisory Mechanism (SSM), or by the relevant banking regulators for Member States not participating in the SSM. The European Securities Markets Authority (ESMA) also has a direct supervision role for certain entities (i.e. credit rating agencies and trade repositories).

(x) Operational risk is a crucial part of prudential regulation and supervision in the financial sector. It covers all operations including the integrity and resilience of their network and information systems. The requirements for these systems are set out in a number of EU regulations, such as the 2013 Capital Requirements Regulation and Directive (CRR/CRD IV). These regulations include requirements on risk management that correspond to, and often exceed, the requirements envisaged under NIS. Although, they do not generally include specific requirements on notification of incidents, such obligations are part of **the Payment Services Directive (PSD2), under which providers of payment services, e.g. credit instutions, must report payment related incidents to the national competent authorities and require the national competent authorities to share these with the EBA and ECB. Further notification requirements are part of** normal supervisory practice in the financial sector and are often included in supervisory manuals. The foregoing should be noted particularly in the context of Article 1(7) of this Directive, concerning explicit obligations on the security of networks and information systems or the notification of incidents in sector-specific Union legal acts.

(x) In various cases the competent supervisory authorities in the financial sector are European institutions, i.e. the European Central Bank; or agencies, i.e. ESMA. In this regard, as noted by the ECB in its Opinion of 25 July 2014 on the NIS proposal, this Directive should be without prejudice to the existing regime for the Eurosystem's oversight of payment and settlement systems, which includes appropriate arrangements, inter alia, in the area of NIS, and the responsibility for developing oversight requirements in the abovementioned areas should remain primarily with these authorities. In turn, these authorities should exchange experiences on matters concerning NIS with the competent authorities for this Directive, pursuant to Article 8a(3)(h). The same consideration applies to non-Eurosystem members of the ESCB exercising such oversight of payment and settlement systems on the basis of national laws and regulations.

		Regulation 648/2012
5. Health sector	Health care settings (including hospitals and private clinics)	- healthcare providers (~~including hospitals~~) as defined in Article 3(g) of Directive 2011/24/EU
6. Drinking water supply and distribution		Supplier and distributor of "water intended for human consumption" as defined in **Article 2(1)(a) of** Council Directive 98/83/EC **but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distribution of commodities and goods.**
7. Digital Infrastructure		Internet exchange points
		Domain name system service providers
		Top Level Domain name registries