COUNCIL OF THE EUROPEAN UNION

Brussels, 16 May 2014

9757/14

Interinstitutional File: 2013/0027 (COD)

TELECOM 111
DATAPROTECT 69
CYBER 27
MI 419
CSC 103
CODEC 1264

NOTE

from:	Presidency
to:	Delegations
No. Cion prop.:	6342/13 TELECOM 24 DATAPROTECT 14 CYBER 2 MI 104 CODEC 313 + ADD1 +ADD2
No. prev. doc.:	7404/14 TELECOM 73 DATAPROTECT 39 CYBER 14 MI 242 CSC 49 CODEC 688
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 *- Draft progress report*

The present report has been drawn up under the responsibility of the Hellenic Presidency. It sets out the work done so far in the Council's preparatory bodies, gives an account of the state of play in the examination of the above mentioned proposal and sets out orientations with a view to the preparation of negotiations with the EP in due course.

PROCEDURAL ASPECTS

1. On 12 February 2013, the Commission submitted its 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* (hereinafter: NIS Directive) with art. 114 TfEU as legal basis.[1] The proposal is part of the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace[2], concerning which the Council adopted conclusions on 25 June 2013.[3] The TTE Councils of 6 June[4] and 5 December[5] took note of the progress made with the examination of the proposal for a NIS Directive.

2. The European Economic and Social Committee[6] and the Committee of the Regions[7] adopted opinions on the proposal on 22 May and on 3-4 July 2013 respectively. The European Parliament adopted in first reading on 13 March 2014 a legislative resolution and a number of 138 amendments, which were drawn up by the internal market (IMCO) committee as the leading committee with the industry (ITRE) and civil liberties (LIBE) committees as 'associated committees'.[8]

1 Doc. 6342/13.
2 Doc. 6225/13.
3 Doc. 11357/13.
4 Doc. 10076/13 and doc. 10457/13.
5 Doc. 16630/13 and doc. 17341/13.
6 TEN/513.
7 2013/C 280/05.
8 Doc. 7451/14.

3. Under the Hellenic Presidency, the Working Group on Telecommunications and the Information Society (WP TELE) continued with an article-by-article examination of the proposal in 6 meetings[9]. On the basis of the discussions in the WP TELE, for which the Presidency had prepared discussion documents[10], and of written comments submitted by most Member States, the Hellenic Presidency has put together the present progress report, which presents the key issues in the proposal and, where possible, identifies where the Member States agree in principle on the line to take. In parallel to this progress report and for illustrative purposes, the Presidency has produced a first amended version of the text of the proposal[11], which was presented to the WP TELE on [XXX] and on the basis of which further work under the Italian Presidency could proceed with a view to engaging with the EP in due course.

SUBSTANCE

Chapter 1: general provisions (articles 1-3):

4. Delegations generally support the proposed subject matter and scope of article 1 ("subject matter") and share the view that the proposed Directive would be an essential part of the EU's overall cyber security strategy. The Presidency believes that a majority of Member States could support some fine-tuning of article 1 along the following lines:

   - *In paragraph 1, the word "ensure" should be replaced with "achieve" in order to reflect that Member States can neither individually nor collectively fully "ensure" a water proof level of NIS.*
   - *Rather than creating a new "cooperation mechanism" between Member States, paragraph 2(b) should build upon existing arrangements to "group" the Member States together to implement the Directive at a strategic/policy level. More concrete operational cooperation could be explored, e.g. in the context of the CERTs[12].*

---

9 On 27/2, 13 and 28/3, 10 and 28/4 and on 21/5 2014.
10 Doc. 7404/14.
11 Doc. [XXX].
12 CERT stands for Computer Emergency Response Team. The point has been raised that, as CERT is a registered EU trademark, there may be a need to use different terminology in the Directive, e.g. Computer Security Incident Response Team (CSIRT).

- *The Member State affected by an incident and/or its CERT should decide whether or not and to which extent relevant information (and possibly personal data) should be shared while taking national security interests and relevant legislation, particularly with regard to the protection of personal data or attacks against information systems, into consideration.*
- *Legal clarification is needed to determine whether the internal market legal base used is appropriate and would allow "public administrations" to be covered by the Directive.*

5. Delegations generally support article 2 ("minimum harmonisation").

6. With regard to the "definitions" in article 3, while noting that these need to be revisited as work progresses, the Presidency believes that delegations generally support the following line:

- *A new definition on "essential services" should be introduced in the list of definitions as this would better allow identifying which actors provide such "essential" services and assessing the risk or "threat" on the security of such services.*
- *The Directive should make reference to a list of common critical infrastructure sectors and provide criteria in order to determine which operators make up these infrastructures. Member States' views still have to become more concrete as regards the level of detail to put in the Directive (and in ANNEX II in particular), such as whether "information society services" and "internet enablers" should be covered by the Directive as well.*
- *The need for the inclusion of additional definitions should be considered further, such as on critical IT services, national plan for risk management, NIS strategy and cooperation plan.*

Chapter II: national NIS frameworks (articles 4-7)

7. Delegations generally support the deletion of article 4 ("principle").

8. With regard to article 5 ("national NIS strategy"), the Presidency has identified broad support for the following orientation:

- *Although the development of a NIS strategy, including a cooperation plan, is supported in principle, the language of this article should focus more on 'future proof', general principles rather than on concrete requirements for the NIS strategy and cooperation plan, as such an approach would best contribute to the building of trust.*

9. With regard to article 6 ("competent authority") and bearing the subsidiarity principle in mind, delegations appear to support an approach which would take due account of the existing practice in Member States:

   - *The Directive should allow Member States sufficient flexibility in designating or maintaining one or several, sector-specific and policy-oriented competent authorities.*
   - *However, Member States should designate a "single contact point".*

10. Regarding article 7 ("CERTs"), Member States generally support the requirement in the Directive to set up or maintain one or several CERTs, which could be the same entity as the "competent authority" or the "single contact point" and agree with the proposed orientations with regard to CERTs as set out in doc. 7404/14, and in particular:

    - *Member States should have sufficient flexibility in terms of technical set-up and financial and human resources of CERTs, which should be reflected in the language of this article and of ANNEX II, but the Directive should nevertheless be firm on the degree of ambition to be achieved and the requirements to be set for CERTs and for the cooperation between them.*

Chapter III: cooperation (articles 8-13)

11. Chapter III of the proposal addresses the architecture for NIS cooperation. According to the Presidency, all Member States acknowledge that through some kind of cooperation, similar, enhanced levels of NIS preparedness could be achieved throughout the EU, which would also facilitate a common and coordinated response to NIS challenges if and where the need arises. Views need to materialise further, however, on how such strategic/policy cooperation network should look like and on what its bearing would be, if at all, on providing coordinated operational responses to national, and possibly cross-border, cyber incidents.

12. With regard to article 8 ("cooperation network"), the Presidency believes that delegations generally support the following approach:

- *The Directive should set out a policy/strategic approach with regard to the cooperation network which, on the one hand, builds upon the capacities to be developed under Chapter II above, while, on the other hand and where appropriate, gives guidance for the working out of detailed modalities for operational cooperation, the latter already being dealt with elsewhere (e.g. ENISA, CERTs).*
- *The focus of a response in case of emergency should be by national capabilities, such as the CERTs and/or competent authorities, and, where necessary in (cross-border) cases yet to be further specified, further voluntary cooperation could take place in an operational cooperation community comprising all the 28 national CERTs with the aim to provide a coordinated EU response.*
- *Peer reviews of capabilities and preparedness by the cooperation network should take place on a voluntary basis*

13. Concerning article 9 ("secure information sharing system"), the Presidency has noted that most Member States are against setting mandatory requirements in the Directive for sharing (commercially sensitive) information in the cooperation network and against the setting up or operation of a dedicated secure infrastructure. Delegations have also raised serious concerns with regard to the proposed role that the Commission would play in this context. Taking the above mentioned into account, the Presidency believes that a re-drafting of this article should be done along the following line:

- *The Directive should not contain any mandatory requirements for the sharing of information and the text of article 9 should reflect this or, alternatively, the article could be deleted, considering that non-sensitive and non-classified information could be exchanged in the cooperation network or relevant information could be exchanged by CERTs.*

14. With regard to article 10 ("early warnings"), delegations appear to be able to support the general orientations set out in doc. 7404/14 and in particular:

- *The provision of early warnings should remain voluntary and the exchange of relevant information in the cooperation network should first of all help boosting the building of trust between the private sector and national competent authorities as well as between national competent authorities.*
- *As the exchange of information on criminal offences regarding attacks on information systems is covered by Directive 2013/40, there is no need for the Directive to address this aspect (i.e. deletion of paragraph 4).*
- *Member States should decide whether and which information to provide to the coordination network (i.e. deletion of paragraph 5).*
- *Early warning should not hamper or delay national actions to handle threats and incidents.*

15. Also with regard to article 11 ("coordinated response"), the Presidency noted broad support for the orientations set out in doc. 7404/14, and in particular:

- *Rather than creating a de facto European competence to coordinate an EU response to (national) incidents, further discussion is needed to clarify when and in which cases a "coordinated EU response" would be needed: in case of major cross-border cyber crises or also in case of more limited day-to-day incidents?*
- *Bearing in mind national competence with regard to security matters, the Directive should build upon existing arrangements to achieve political coordination at EU level in case of large-scale cyber crises rather than putting in place new and potentially slow mechanisms.*
- *In addition to political coordination at EU level, the Directive should facilitate technical/practical cooperation (e.g. amongst CERTs), where further requirements for an operational response to cyber crises could be developed.*

16. The Presidency notes that, although Member States' final position on article 12 ("Union NIS plan") will be subject to the outcome on articles 8-11, most delegations could support that the following approach be accommodated in the text of the proposal:

- *The Directive could set out a Union NIS "framework" for cooperation rather than a "plan", which is focussed on policy coordination and development, which fully uses the relevant expertise of ENISA and which would be regularly reviewed by the cooperation network set up under article 8.*
- *The cooperation "framework" should cover topics such as modalities for CERT-to-CERT communications, exchange of best practices, awareness raising and exercises and training, and benefit from ENISA's expertise in this regard.*

17. With regard to article 13 ("international cooperation"), the Presidency noted the Member States' wish for the text to reflect that all participating members in the cooperation framework should agree to the participation of third countries or international organisations in that framework.

Chapter IV: security of networks (articles 14-16), Chapter V: final provisions (articles 17-23) and Annexes I and II: CERTs and market operators

18. With regard to article 14 ("security requirements and incident notification"), the Presidency noted that those Member States, where a national practice of voluntary notification has achieved satisfactory cooperation between stakeholders and public authorities, would prefer the Directive to build on this experience. Other Member States question whether in addition to this, requirements for mandatory reporting should be introduced. All Member States agree that further clarification is needed as regards the various notification requirements, which exist under various pieces of EU legislation. In view of the above, the Presidency would recommend the following approach:

- *The Directive could set out mandatory reporting requirements in case of incidents having a significant cross-border impact involving several Member States.*
- *In case of internal incidents with a limited impact, Member States should have flexibility to determine, in accordance with article 2, whether and how to report at a national level .*

- *The Directive should set out the parameters for determining the impact of (sector-specific) incidents but it would be up to the Member States on the basis of those parameters to decide whether a specific incident should be reported.*
- *Member States should have flexibility on the modalities for reporting to sector-specific competent authorities, which, in turn, may report to the national "single contact point".*

19. Regarding article 15 ("implementation and enforcement"), and based on the views from delegations, the Presidency proposes that:

- *The Directive should provide sufficient scope for national solutions with the aim to involve the private sector more than currently proposed, e.g. with regard to security audits, development of technical capabilities, training courses, etc.*
- *The Directive should make provision to also allow, where appropriate, for multiple, sector-specific competent authorities, which also have implementation and enforcement responsibilities.*

20. As regards the issue of "standardisation" under article 16, the Presidency concludes that delegations do not see an immediate need for a redrafting of the article.

21. Regarding article 17 ("sanctions") and paragraph 2 in particular, further consideration is needed in order to further clarify the link between the NIS Directive and the forthcoming Data Protection Regulation.

22. Finally, the Presidency noted that delegations wish to come back at a later point in time on the "transposition period" and the "entry into force" (articles 21 and 22) and that the finalisation of ANNEX I regarding the scope tasks and requirements of CERTs ANNEX II regarding the sectors and entities to be covered in an "exhaustive" or "indicative" list will need to be revisited later, subject to the negotiations on the substance of the articles of the proposal.

CONCLUSION

23. The Hellenic Presidency has noted that, without exception, all Member States are well aware of the urgent need to improve network and information security and to take action in this regard at EU level. In this context, Member States have given the examination of the Commission's proposal their utmost attention and considerable progress has been made in recent months in identifying the direction in which the proposal should develop further, as explained above.

24. Regarding the provisions related to Chapters I, II and IV and on the basis of the discussions in the Council's preparatory bodies, the Presidency believes that the proposed orientations and conclusions in this progress report should be a sufficient basis for developing the proposal further under the incoming Italian Presidency. These orientations and conclusions were put together bearing in mind the need to strike the right balance between improving cyber-security, building the necessary trust and, for the sake of efficiency, making full use of existing experience as well as avoiding duplication of the expertise of existing bodies and mechanisms.

25. Concerning chapter III, as noted above (paragraph 11), Member States do agree on the need to strengthen strategic/policy cooperation on NIS at EU level. A number of Member States believe that the Directive should provide for more specific criteria and requirements for operational cooperation in case of NIS incidents. Most Member States, however, see strategic/policy cooperation as a first priority for building the necessary trust while, at the same time, modalities for operational cooperation could be further worked out in the context of existing mechanisms and bodies. As proposed above (paragraphs 11-17), the Presidency does not see strategic/policy cooperation and operational cooperation as mutually exclusive options but believes that the priority in the Directive should be on strategic/policy cooperation while at the same time giving guidance to existing bodies and mechanisms with regard to operational cooperation.

*

* *

Following Coreper's consideration of this progress report on 28 May, the Presidency will present it to the Council with the invitation to take note of it.