COUNCIL OF
THE EUROPEAN UNION

Brussels, 22 November 2013

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

16630/13

**TELECOM 322
DATAPROTECT 178
CYBER 33
MI 1064
CODEC 2676**

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.:	16333/13 TELECOM 313 DATAPROTECT 170 CYBER 30 MI 1039 CODEC 2717
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 - *Progress report*

The present report has been drawn up under the responsibility of the Lithuanian Presidency. It sets out the work done so far in the Council's preparatory bodies and gives an account of the state of play in the examination of the above mentioned proposal.

PROCEDURAL ASPECTS

1. On 12 February, 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 was 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 Council of 6 June 2013 took note of the progress made with the examination of the proposal for a NIS Directive.[4]

2. The European Economic and Social Committee[5] and the Committee of the Regions[6] adopted opinions on the proposal on 22 May and on 3-4 July respectively. In the European Parliament, the internal market (IMCO) committee is the leading committee with the industry (ITRE) and civil liberties (LIBE) committees as 'associated committees'. In terms of timing, the LIBE committee is planning to take a vote in November, ITRE in December and IMCO is planning to adopt a report and a set of amendments on 22-23 January 2014.

3. Under the Lithuanian Presidency, the Working Group on Telecommunications and the Information Society (WP TELE) examined the proposal in 5 meetings[7]. As many delegations were only able to express preliminary views and maintained scrutiny reservations on (parts of the) text, it has not been possible for the Lithuanian Presidency to attach a revised text to this progress report. However, in the discussions, delegations raised a number of key issues and concerns, as set out below, which will need to be reflected in a revision of the text of the proposal.

[1] Doc. 6342/13.

[2] Doc. 6225/13.

[3] Doc. 11357/13.

[4] Doc. 10076/13 and doc. 10457/13.

[5] TEN/513.

[6] 2013/C 280/05.

[7] On 18/7, 26/9, 8/10, 5/11 and 19/11/2013.

SUBSTANCE

4. A general description of the main elements of the proposed NIS Directive was given in the progress report for the June TTE Council.[8] Although all delegations fully acknowledge the need for action to face NIS incidents and curb cyber attacks, views differ as to how best to ensure network security throughout the EU. Whereas some delegations confirm in the article-by-article examination of the proposal that they would prefer a flexible approach, with EU-wide binding rules limited to critical infrastructure and basic requirements, complemented by optional, voluntary measures, other delegations as well as the Commission consider that only legally binding measures would bring about the necessary EU security levels. This difference in philosophy explains the differences in positions taken on the detailed provisions in the proposal, as explained below.

5. *NIS strategy and NIS competent body*: in view of the objective to have in place a minimum level of capability to prevent, handle and respond to risks and incidents affecting information systems, EU Member States would be required to adopt national NIS strategies, designate national competent authorities on NIS, and set up computer emergency response teams (CERTs) for NIS.

   Delegations acknowledge that a substantial disruption in one Member State can also affect other Member States and could support the principle of a coordinating entity at national level. However, in particular those Member States, which already adopted NIS strategies, designated competent bodies and set up a national CERT, seem to critically look at chapter II of the proposal, which deals with the *national framework on NIS:* they wish to make sure that the requirements that will have to be met by Member States are consistent with and do not go beyond the current national practice. Some delegations believe that the competent body should be a contact point and delegate tasks to national regulators, which have the necessary sector-specific expertise. This should also ensure that the imposed requirements are in accordance with national security provisions. Some delegations point out that more confidence-building measures are needed in order to build trust, rather than putting the focus on administrative and bureaucratic arrangements.

[8] Doc. 10076/13.

Other delegations seek further clarification about the terminology used in this chapter, such as 'risks' and 'threats' and wonder what the exact requirements are and also question whether these requirements should only concern the private sector or also the public sector. With regard to the competent authority and its task description, many issues require further clarification, such as whether the authority should assume operational tasks, which is something many Member States object to, and what should be the division of responsibilities with the national CERT.

6. *Risk management and incident notification*: 'market operators' and public administrations should properly assess the risks posed to their information systems, take appropriate measures to prevent and deal with incidents and report any serious incident having a significant impact on the core services provided to the competent authorities.

   On chapter IV of the proposal on *security of networks and information systems of public administrations and market operators*, several delegations doubt whether in addition to 'operators of critical infrastructures', also 'information society service providers' should be covered by the proposal. This concern about scope is closely linked to the definition of ‘market operators’ in Chapter I and the non-exhaustive list in Annex II. Many delegations called for more clarity on the definition and for more flexibility for Member States to define which sectors constitute national critical infrastructures. Some delegations wish to limit the proposed requirements to the private sector only and others call for the security breach reporting requirements in this chapter to be voluntary in line with current national practices. The question is also raised why hardware/software manufacturers and micro enterprises are not covered and Member States also have concerns about the consistency of the proposed notification requirements related to security breaches with those in other pieces of EU legislation, such as in the regulatory framework for electronic communications, as a result of which providers of electronic communications networks or services or trust service providers are not subject to the requirements of the current proposal. In general, many delegations question whether or how Member States could actually "ensure" that parties secure their networks and notify incidents; in this regard, the appropriateness of Article 114 TfEU as a legal basis has been brought up as an issue for clarification. There are also concerns with regard to the implications of notifications on matters of privacy and confidentiality of information.

7. *Cooperation network*: in order to ensure a coordinated response to incidents, where necessary, a cooperation network on NIS risks and incidents should be created to allow permanent communication between the Commission and the 28 competent authorities.

   Chapter III of the proposal on *cooperation between competent authorities* will require further examination. Further discussion will be needed on the tasks of the cooperation network although many delegations are of the opinion that it should not assume any operational tasks; some argue in this respect that it would be better to refer to a *mechanism* rather than to a *network.* A number of organisational issues also require further clarification, such as who will chair the cooperation network, what its costs would be, and what the relationship and division of responsibilities would be with the cooperation of national CERTs with ENISA and with Europol. Some delegations argue that the sharing of information in the network should be done on a voluntary basis and question the need for the proposed and dedicated 'secure information-sharing system'. The proposed early warning mechanism raises many queries and concerns, e.g. which information shall be shared at what point in time and with what possible consequences for the incident or risk. Also, many Member States question the scope of the proposed coordinated response mechanism, and call for a framework of cooperation on NIS rather than an operational incident response plan. When and under what conditions a coordinated response would be required requires further discussion.

8. With regard to the two chapters I and V of the proposal, i.e. the *general provisions* (which were examined under the Irish Presidency) and the *final provisions* respectively, a first general exchange of views took place but some provisions will need to be revisited for further consideration, such as; the application of the proposed security requirements in relation to those in the Framework Directive (2002/21/EC); the definitions of 'risk', 'incident' and 'market operator' (in connection with Annex II *List of market operators*); enforcement (such as notification of incidents to the police); standardisation; implementing acts (all delegations opposed the use of delegated acts in this field of work) and the transposition period (for the transposition into national law as well as for the publication of the national NIS strategy).

OUTLOOK

9. The article-by-article examination of the proposal shows that delegations are seeking from the Commission clarification on, but also justification for, the proposed measures as compared to the current national situations and (national and international) voluntary incident reporting and cooperation mechanisms, such as those which exist within European and international CERT communities (such as the European Government CERT Group) and which could encompass the facilitation role of ENISA. In the further examination of the proposal in the WP TELE, it appears that the main challenge will be to agree on an approach, which strikes the right balance between EU-wide binding rules and optional, voluntary measures, all of which should lead to similar levels of NIS preparedness among the Member States and allow the EU to respond effectively to NIS challenges.

10. Delegations are most welcome to provide the Presidency with further drafting suggestions, which will be given due consideration in the further examination of the proposal.

*

*   *

Following its consideration by Coreper on 27 November, the Presidency presents this progress report to Council with the invitation to take note of it.