Comments and Questions by Germany regarding the Impact Assessment and Art. 3 and 4 NIS2

Please note: The following list of comments and questions regarding the Impact Assessment and Art. 3 and 4 NIS2 is non-exhaustive and may be expanded in future discussions. Comments and questions are sorted by priority.

1. Comment regarding Art. 4 no. 23 – Under the proposed wording, the complete public administration of Germany – including the federal-, state- and partly communal-levels – would be within the scope of NIS2. As already mentioned in our comment regarding Art. 2 para. 2 (b) and after further review, Germany proposes to **exclude** "**entities of public administration**" **entirely** from the scope of application of NIS2 and rather define secure gateways or central points of contact for the public administrations at the national level. The latter was already the case for the current NIS directive (e.g. cooperation via CERTs). This proposal is mainly based on three aspects:

   (1) Organization and information security management of the public administration within a member state is a matter of internal and national security. Therefore, the proposed wording **intervenes disproportionately into the competencies of the member states**.

   (2) Furthermore, according to our assessment, **Art. 114 TFEU** (functioning of the internal market) **does not provide for a sufficient legal basis** for the extension of the scope of application of NIS2 to entities of public administration. Germany would like to refer to the discussions, which lead to the exclusion of "entities of public administration" from the scope of application in the current NIS directive.

   (3) And finally, the exclusion of entities "*that carry out activities in the areas of public security, law enforcement, defence or national security*" is in our view unable to deal with the different **complex and intertwined cyber-structures of public administrations**.

2. Question regarding Art. 4 no. 5 – The **definition of "incident"** has significantly changed in comparison to Art. 4 no. 7 of the current NIS directive. Currently, "*'incident' means any event having an actual adverse effect on the security of network and information systems*". The proposal defines it the following way: "'*incident' means any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems*". In the energy sector for example, even a high network load would affect the availability of data and would, therefore, constitute an "incident". Kindly explain the Commissions rationale behind this new definition, possibly in the context of Art. 20 para. 2 that stipulates an immediate reporting obligation.

3. Comment regarding Art. 4 no. 13 – The **definition of "domain name system (DNS)"** appears misleading in our view. Germany proposes to change the definition to: "'*domain name system (DNS)' means a hierarchical distributed ~~naming~~ directory system which ~~allows end-users to reach services and resources on the internet~~ primarily serves for name resolution in IP addresses*".

4. Comment regarding Art. 4 no. 19 – The **definition of "cloud computing service"** is derived from the NIST definition. Germany proposes to use the of the ISO 17788 definition of "cloud computing" instead: "*Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.*". Germany's proposal is based on two reasons:

   (1) Within NIS2 itself, reference is made to the corresponding ISO standard and, in addition, the draft of the European Cybersecurity Certification Scheme for Cloud Services (EUCS) also uses the above-mentioned definition. If EUCS will be used for a possible regulation of cloud service providers, the definition used in NIS2 should be congruent.

   (2) NIST was the first definition of its kind and pioneering in nature. During the development of ISO standards, further definitions became necessary and thus ISO 17788 was created, which of course takes the NIST definition into account and does not contradict it. ISO 17788 is thus a whole system of coordinated definitions around cloud computing.

5. Question regarding Art. 4 no. 22 – Under the current **definition of "social networking services platform"** internet messengers (e.g. WhatsApp) would in our view fall within the definition as well. Is such inclusion of internet messengers intended by the Commission? If not, a clear delineation should be added.

6. Question regarding Art. 4 – Has the Commission assessed the question whether to include definitions for the terms "**operators of ground-based infrastructure**" (*cf*. Annex 1) or "**assets**" (*cf*. Art. 5 para. 1 (c))?

Council of the European Union
General Secretariat

Interinstitutional files:
2020/0359(COD)

Brussels, 17 February 2021

WK 1627/2021 ADD 6

LIMITE

CYBER
JAI
DATAPROTECT
TELECOM
MI
CSC
CSCI

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Delegations
Subject:	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 - Comments by DE

Delegations will find in Annex comments by DE on the above-mentioned subject.