Council of the European Union
General Secretariat

Interinstitutional files:
2017/0225 (COD)

Brussels, 17 May 2018

WK 5902/2018 INIT

LIMITE

CYBER
TELECOM
CODEC
COPEN
COPS
COSI
CSC
CSCI
IND
JAI
JAIEX
POLMIL
RELEX

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:	Polish delegation
To:	Horizontal Working Party on Cyber issues
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") - Comments from the Polish delegation on Articles 45 and 46

Delegations will find in Annex the comments of the Polish delegation on Articles 45 and 46 of the above mentioned proposal.

ANNEX

Article 45

Security objectives for ICT processes, products and services

1. ICT processes, products and services subject to European cybersecurity certification shall be developed, implemented, operated, maintained and finally disposed as to achieve, , as applicable, **at least** the following security objectives:

   (1) protect data stored, transmitted or otherwise processed against accidental or unauthorised storage, processing, access or disclosure **during the entire process, product or service lifecycle**;

   (2) protect data stored, transmitted or otherwise processed against accidental or unauthorised destruction, loss or alteration **or lack of availability during the entire process, product or service lifecycle**;

   (3) authorised persons, programmes or machines can access exclusively the data, services or functions to which their access rights refer;

   (4) record which data, functions or services have been ~~communicated~~ **accessed, used or otherwise processed**, at what times and by whom;

   (5) it is possible to check which data, services or functions have been accessed**,** used **or otherwise processed**, at what times and by whom;

   (6) restore the availability and access to data, services and functions in a timely manner in the event of physical or technical incident;

   (7) software **and hardware are timely updated** that **do** not contain **publicly known** vulnerabilities, and are provided mechanisms for secure updates**;**

2. **ICT processes and services are developed and operated <u>and ICT products are manufactured</u> according to the security requirements stated in the particular scheme, characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of, or to prevent cybersecurity incidents.**

Article 46

Assurance levels of European cybersecurity certification schemes

1. A European cybersecurity certification scheme may specify one or more of the following assurance levels: basic**<consider, if "foundation/fundamental" is better word, as suggested in the UK proposal sent to HWP at the beginning of May>**, substantial and/or high, for ICT **processes,** products and services. **<u>The level of assurance shall be commensurate with the level of the risk associated with the use or application in specific environment of an ICT process, product or service.</u>**
2. **A European cybersecurity certificate shall refer to a defined** assurance level. A EU statement of conformance shall applied to assurance level "basic". **<to be discussed>**
3. The assurance levels: basic, substantial and high shall refer to the corresponding degree of effort for the evaluation that **<u>security requirements including security functionalities of an</u> ICT process, product or service are met.**

4. **The corresponding degree** of effort for the evaluation shall mean the following:
    a. for assurance level **"**basic**"** - at least:
        i. reviewing of a technical documentation for completeness and accuracy, in particular to check whether security problem as well as countermeasures to respond to this problem are defined,
        ii. checking if a quality management system is operated and used to analyse risks and ensure that risks are met in adequate manner,
        iii. checking if procedures are in place to update the ICT process, product or service, if new vulnerablilities are detected.
    b. assurance level **"**substantial**"** shall include all activities for assurance level "basic" and at least:
        i. confirming non-applicability of **publicly known vulnerabilities and attack techniques by** performing cyberattacks requiring potential equivalent to these carried out by actors **with limited skills and resources,**
        ii. testing of correct implementation and effectiveness of the necessary security functionality against publicly known vulnerabilities,
        iii. ensuring that the vendor shall make an assessment of the root cause of each vulnerability or other security relevant weakness found during evaluation and demonstrate countermeasures taken that prevents such vulnerability may occur in the certified ICT processes, products or services in the future.
    c. assurance level **"**high**"** shall include all activities for assurance level "substantial" and at least:
        i. confirming non-applicability of **potential vulnerabilities by** performing state-of-art cyberattacks, as defined in technical specifications and agreed in respective scheme, requiring potential equivalent to these carried out by actors **with significant skills and resources, via penetration testing**
        ii. testing of correct implementation and effectiveness of the necessary security functionality against potential vulnerabilities.

5. **European cybersecurity certification scheme shall adopt and use an evaluation methodology based on standards, technical specifications, agreed processes and procedures.**
6. **European cybersecurity certification scheme may specify several evaluation levels depending on the rigour, scope and depth of the evaluation methodology. ~~Each one of the evaluation levels shall correspond to one of the assurance levels and be defined by an appropriate combination of assurance components.~~**