EUROPEAN
COMMISSION

Brussels, 13.9.2017
COM(2017) 477 final

ANNEX 1

ANNEX

to the

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'')

{SWD(2017) 500 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES

Conformity assessment bodies that wish to be accredited shall meet the following requirements:

1. A conformity assessment body shall be established under national law and have legal personality.

2. A conformity assessment body shall be a third-party body independent of the organisation or the ICT products or services it assesses.

3. A body belonging to a business association or professional federation representing undertakings involved in the design, manufacturing, provision, assembly, use or maintenance of ICT products or services which it assesses, may, on condition that its independence and the absence of any conflict of interest are demonstrated, be considered a conformity assessment body.

4. A conformity assessment body, its top-level management and the personnel responsible for carrying out the conformity assessment tasks shall neither be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the ICT product or service which is assessed, nor shall it be the authorised representative of any of those parties. This shall not preclude the use of assessed products that are necessary for the operations of the conformity assessment body or the use of such products for personal purposes.

5. A conformity assessment body, its top-level management and the personnel responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, manufacture or construction, the marketing, installation, use or maintenance of those ICT products or services, or represent the parties engaged in those activities. They shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to conformity assessment activities for which they are notified. This shall apply, in particular, to consultancy services.

6. Conformity assessment bodies shall ensure that the activities of their subsidiaries or subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities.

7. Conformity assessment bodies and their personnel shall carry out the conformity assessment activities with the highest degree of professional integrity and the requisite technical competence in the specific field and shall be free from all pressures and inducements, including of a financial nature, which might influence their judgement or the results of their conformity assessment activities, especially as regards persons or groups of persons with an interest in the results of those activities.

8. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks assigned to it under this Regulation, whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility.

9. At all times and for each conformity assessment procedure and each kind, category or sub-category of ICT products or services, a conformity assessment body shall have at its disposal the necessary:

(a) personnel with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks;

(b) descriptions of procedures in accordance with which conformity assessment is carried out, ensuring the transparency of those procedures and the possibility of reproducing them. It shall have in place appropriate policies and procedures that distinguish between tasks that it carries out as a notified body and other activities;

(c) procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the ICT product or service technology in question and the mass or serial nature of the production process.

10. A conformity assessment body shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner, and shall have access to all necessary equipment and facilities.

11. The personnel responsible for carrying out conformity assessment activities shall have the following:

(a) sound technical and vocational training covering all the conformity assessment activities;

(b) satisfactory knowledge of the requirements of the assessments they carry out and adequate authority to carry out those assessments;

(c) appropriate knowledge and understanding of the applicable requirements and testing standards;

(d) the ability to draw up certificates, records and reports demonstrating that assessments have been carried out.

12. The impartiality of the conformity assessment bodies, of their top-level management and of the assessment personnel shall be guaranteed.

13. The remuneration of the top-level management and of the assessment personnel of a conformity assessment body shall not depend on the number of assessments carried out or on the results of those assessments.

14. Conformity assessment bodies shall take out liability insurance unless liability is assumed by the State in accordance with national law, or the Member State itself is directly responsible for the conformity assessment.

15. The personnel of a conformity assessment body shall observe professional secrecy with regard to all information obtained in carrying out their tasks under this Regulation or pursuant

to any provision of national law giving effect to it, except in relation to the competent authorities of the Member States in which its activities are carried out.

16. Conformity assessment bodies shall meet the requirements of standard EN ISO/IEC 17065:2012.

17. Conformity assessment bodies shall ensure that testing laboratories used for conformity assessment purposes meet the requirements of standard EN ISO/IEC 17025:2005.