



**CEPIS**  
Council of European Professional  
Informatics Societies

The Council of European Professional  
Informatics Societies  
Avenue Roger Vandendriessche 18  
B-1150 Brussels, Belgium  
Tel. +32 2 772 18 36

Brussels, 14 March 2018

### **New regulation on European Union Network and Information Security Agency (ENISA)**

*To whom it may concern*

CEPIS, representing more than 450.000 ICT and informatics professionals in 31 European member societies, very much welcomes the initiative to reform the European Union Network and Information Security Agency (ENISA). Indeed, so much depends on information and communication systems that their secure functioning is a key concern and the new initiative on cybersecurity certification of ICT products and services is of utmost importance.

The CEPIS Legal and Security Issues Special Interest Network has reviewed the Commission's proposal (COM(2017) 477 final) and I would like to point out some amendments to improve ENISA's effectiveness and efficiency, especially with regard to certification but also in general:

- (1) The ENISA Management Board (MB) should have (again) Stakeholder Representatives (please cf. detailed proposals on Recital 40 and Article 13 in the annex). Having Stakeholder Representatives at the table at every meeting of the MB (not just at occasional invitations) is essential for a qualified discussion and European perspective on the core matters of ENISA. This could also be seen in comparing the periods till 2013 (with Stakeholder Representatives) and from 2013 (without Stakeholder Representatives). The Stakeholder Representatives in the MB were important as they delivered valuable input to the work of ENISA on a more strategic level than the Permanent Stakeholders' Group (PSG) has the opportunity to do. For instance, the MB has been able to accompany the development of the annual Work Programme of ENISA more closely and consistently than the PSG set-up permits the PSG members to do. The Stakeholder Representatives in the MB also have the opportunity to interact with the Member State representatives in the MB in direct discussion in the later stages of the development of the annual Work Programme.
- (2) In addition, ENISA's new tasks on certification make it essential to include a representative of the European Standardisation Organisations (ESO) into the list of Stakeholder Representatives in the MB (please cf. the detailed proposals on Recital 40 and Article 13 in the annex).



**CEPIS**  
Council of European Professional  
Informatics Societies

- (3) In the attached proposal for Article 13 the four Stakeholder Representatives have voting rights, which the three representatives back in 2004 did not have. The voting rights may be negotiable, but the representation is essential.
  
- (4) A Standardisation and Certification Stakeholders' Group needs to be established in addition to the Permanent Stakeholder's group (PSG), but with a different composition, as the composition of both groups needs to be different to enable them doing their tasks (please cf. the detailed proposals on Recital 44 bis and on Articles 13 and 20 a bis in the annex). Practically the PSG needs to be composed in a way, that it enables influence on the main Management Board members (representatives from the member states). This can also be seen in the current composition of the PSG, that has a large proportion (two thirds) of industry representatives, as they are the ones that seem to be most important for the Management Board most (due to the relation to economic growth, employment and similar issues in member states). The PSG composition does however not reflect the needs for a balanced representation of different stakeholders in standardisation and certification (e.g. consumers of certification results, providers of products and services for certification, evaluators, certifiers), that is essential for credibility and trust of standardisation and certification results. Hence a dedicated Standardisation and Certification Stakeholders' Group is needed.

The attached document includes the proposal for amendments as a synopsis in tabular form. We would be more than happy to discuss these issues in more detail. Also Prof. Dr. Kai Rannenber as the Chair of the CEPIS Legal and Security Issues Network is happily available via [kai.rannenber@cepis.org](mailto:kai.rannenber@cepis.org).

Yours sincerely,

---

Byron Nicolaides  
President

*The Council of European Professional Informatics Societies (CEPIS) <https://www.cepis.org/> is a non-profit organisation seeking to promote best practice for IT professionals and users throughout Europe. CEPIS represents over 450,000 ICT and informatics professionals in 31 countries. CEPIS focusses on four pillars of activity: promoting high standards for IT professionals, growing the pool of future IT professionals, promoting digital competence for the workforce, and making IT good for Europe.*



## Proposal for amendments

### Recital 40

Current wording	Proposed amendment
<p>The Management Board, <b>composed of</b> the Member States and the Commission, should define the general direction of the Agency's operations and ensure that it carries out its tasks in accordance with this Regulation. The Management Board should be entrusted with the powers necessary to establish the budget, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for decision making by the Agency, adopt the Agency's Single Programming Document, adopt its own rules of procedure, appoint the Executive Director and decide on the extension of the Executive Director's term of office and on the termination thereof.</p>	<p>The Management Board, <b>representing</b> the Member States and the Commission <b>as well as stakeholders relevant for the Agency's mission</b>, should define the general direction of the Agency's operations and ensure that it carries out its tasks in accordance with this Regulation. The Management Board should be entrusted with the powers necessary to establish the budget, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for decision making by the Agency, adopt the Agency's Single Programming Document, adopt its own rules of procedure, appoint the Executive Director and decide on the extension of the Executive Director's term of office and on the termination thereof. <b>In the light of the highly technical and scientific mission and tasks of the Agency, it is appropriate for the Management Board to consist of members with a high level of expertise in issues within the scope of the Agency's mission appointed by the Council and Commission.</b></p>

### New Recital 44 bis

Current wording	Proposed amendment
	<p><b>The Agency should have a Standardisation and Certification Stakeholders' Group as an advisory body, to ensure regular dialogue with the European Standardisation Organisations and the stakeholders therein, e.g. European Standardisation Organisations the private and the public sector (with both providers and users of network and information security), consumers' organisations, academic experts in network and information security and other relevant</b></p>



	<p><b>stakeholders. The Standardisation and Certification Stakeholders' Group, set up by the Management Board on a proposal by the Executive Director, should focus on issues relevant to standardisation and certification and bring them to the attention of the Agency. The composition of the Standardisation and Certification Stakeholders' Group and the tasks assigned to this group, to be consulted in particular regarding the draft Work Programme, should ensure sufficient representation of stakeholders in the work of the Agency related to Standardisation and Certification.</b></p>
<p><b>Justification</b></p> <p>The Standardisation and Certification Stakeholders' Group needs to be established in addition to the Permanent Stakeholder's group (PSG), but with a different composition. Practically the PSG needs to be composed with a very strong industry representation. This can also be seen in the current composition of the PSG that has a large proportion (two thirds) of industry representatives, due to the relation to economic growth, employment etc. The PSG composition does however not reflect the needs for a balanced representation of different stakeholders in standardisation and certification (e.g. consumers of certification results, providers of products and services for certification, evaluators, certifiers), that is essential for credibility and trust of standardisation and certification results. Hence a dedicated Standardisation and Certification Stakeholders' Group is needed.</p>	

## Article 12

<b>Current wording</b>	<b>Proposed amendment</b>
<p>The administrative and management structure of the Agency shall be composed of the following:</p> <p>(a) a Management Board which shall exercise the functions set out in Article 14;</p> <p>(b) an Executive Board which shall exercise the functions set out in Article 18;</p> <p>(c) an Executive Director who shall exercise the responsibilities set out in Article 19; <b>and</b></p> <p>(d) a Permanent Stakeholders' Group which shall exercise the functions set out in Article 20.</p>	<p>The administrative and management structure of the Agency shall be composed of the following:</p> <p>(a) a Management Board which shall exercise the functions set out in Article 14;</p> <p>(b) an Executive Board which shall exercise the functions set out in Article 18;</p> <p>(c) an Executive Director who shall exercise the responsibilities set out in Article 19;</p> <p>(d) a Permanent Stakeholders' Group which shall exercise the functions set out in Article 20; <b>and</b></p> <p><b>(e) a Standardisation and Certification Stakeholders' Group which shall exercise the functions set out in Article 20a.</b></p>



**Justification**

The Standardisation and Certification Stakeholders' Group needs to be established in addition to the Permanent Stakeholder's group (PSG), but with a different composition. Practically the PSG needs to be composed with a very strong industry representation. This can also be seen in the current composition of the PSG that has a large proportion (two thirds) of industry representatives, due to the relation to economic growth, employment etc. The PSG composition does however not reflect the needs for a balanced representation of different stakeholders in standardisation and certification (e.g. consumers of certification results, providers of products and services for certification, evaluators, certifiers), that is essential for credibility and trust of standardisation and certification results. Hence a dedicated Standardisation and Certification Stakeholders' Group is needed.

**Article 13**

<b>Current wording</b>	<b>Proposed amendment</b>
<p>1. The Management Board shall be composed of one representative of each Member State, and two representatives appointed by the Commission. All representatives shall have voting rights.</p>	<p>1. The Management Board shall be composed of one representative of each Member State, two representatives appointed by the Commission, <b>as well as four representatives, proposed by the Commission and appointed by the Council, each of whom represents one of the following groups:</b></p> <ul style="list-style-type: none"> <li><b>(a) information and communication technologies industry;</b></li> <li><b>(b) consumer groups;</b></li> <li><b>(c) academic experts in network and information security;</b></li> <li><b>(d) European Standardisation Organisations.</b></li> </ul> <p>All representatives shall have voting rights.</p>
<p><b>Justification</b></p> <p>This composition reflects the original setting for ENISA amended by an additional representative of the European Standardisation Organisations. Having Stakeholder Representatives at the table at every meeting of the Management Board (not just at occasional invitations) is essential for a qualified discussion and European perspective on the core matters of ENISA. The Stakeholder Representatives in the Management Board were important as they delivered valuable input to the work of ENISA on a more strategic level than the Permanent Stakeholders' Group (PSG) has the opportunity to do. For instance, the Management Board has been able to accompany the development of the annual Work Programme of ENISA more closely and consistently than the PSG set-up permits the PSG members to do. The Stakeholder Representatives in the Management Board would also have the opportunity to</p>	



interact with the Member State representatives in the Management Board in direct discussion in the later stages of the development of the annual Work Programme.

In addition, ENISA's new tasks on certification make it essential to include a representative of the European Standardisation Organisations (ESO) into the list of Stakeholder Representatives in the Management Board.

In this proposal the four Stakeholder Representatives have voting rights, which the three representatives back in 2004 did not have. The voting rights may be negotiable, but the representation is essential.

#### **New Article 20 a bis**

<b>Current wording</b>	<b>Proposed amendment</b>
New	<ol style="list-style-type: none"><li><b>1. The Management Board, acting on a proposal by the Executive Director, shall set up a Standardisation and Certification Stakeholders' Group composed of recognised experts representing the relevant stakeholders in ICT Security Standardisation and Certification, such as European Standardisation Organisations, the private and the public sector (with both providers and users of network and information security), consumers' organisations, academic experts in network and information security and other relevant stakeholders.</b></li><li><b>2. Procedures for the Standardisation and Certification Stakeholders' Group, in particular regarding the number, composition, and the appointment of its members by the Management Board, the proposal by the Executive Director and the operation of the Group, shall be specified in the Agency's internal rules of operation and shall be made public.</b></li><li><b>3. The Standardisation and Certification Stakeholders' Group shall be chaired by the Executive Director or by any person the Executive Director appoints on a case-by-case basis.</b></li><li><b>4. The term of office of the Standardisation and Certification Stakeholders' Group's members shall be two-and-a-half years. Members of the Management Board may not be members of the Standardisation and Certification Stakeholders' Group. Experts</b></li></ol>



	<p><b>from the Commission and the Member States shall be entitled to be present at the meetings of the Standardisation and Certification Stakeholders' Group and to participate in its work. Representatives of other bodies deemed relevant by the Executive Director, who are not members of the Standardisation and Certification Stakeholders' Group, may be invited to attend the meetings of the Standardisation and Certification Stakeholders' Group and to participate in its work.</b></p> <p><b>5. The Standardisation and Certification Stakeholders' Group shall advise the Agency in respect of the performance of its activities. It shall in particular advise the Executive Director on drawing up a proposal for the Agency's work programme on Standardisation and Certification and on ensuring communication with the relevant stakeholders on all issues related to that part of the work programme.</b></p>
<p><b>Justification</b></p> <p>The Standardisation and Certification Stakeholders' Group needs to be established in addition to the Permanent Stakeholder's group (PSG), but with a different composition. Practically the PSG needs to be composed with a very strong industry representation. This can also be seen in the current composition of the PSG that has a large proportion (two thirds) of industry representatives, due to the relation to economic growth, employment etc. The PSG composition does however not reflect the needs for a balanced representation of different stakeholders in standardisation and certification (e.g. consumers of certification results, providers of products and services for certification, evaluators, certifiers), that is essential for credibility and trust of standardisation and certification results. Hence a dedicated Standardisation and Certification Stakeholders' Group is needed.</p>	