Brussels, 8 February 2018

For flexible and market relevant cybersecurity compliance and certification schemes

Orgalime comments on the Commission proposal for a Regulation on a "Cybersecurity Act" (COM(2017) 477 final)[1]

EXECUTIVE SUMMARY

Scope and definitions

- The scope of application and the **definition of ICT products and services** should clarify that these are intended **to be connected to the Internet** to be covered by certification schemes.

Nature of certification

- **Third-party certification** is not always appropriate to promote cybersecurity in the market. By experience, private contracts applying to professional products (B2B) combined with the use of standards **and alternative conformity assessment procedures** often provide **more adequate**, cost-efficient and flexible answers to manufacturers, especially SMEs.

- **Self-declaration of conformity** in particular is an established and a **well-functioning conformity assessment procedure** which should be included as an option where a minimum level of cybersecurity for certain categories of ICT products is required.

- The Cybersecurity Act should ensure that future schemes **follow a risk-based approach**, depending on the context and severity of the situation, taking due consideration for the cybersecurity-by-design concept.

- All future European cybersecurity compliance and certification schemes should remain of **voluntary application** as certain market factors could jeopardise the voluntary nature of future compliance and certification schemes.

- The access of the European industry to the international markets is key for the success of a European digital single market. Therefore, the Cybersecurity Act should acknowledge that

[1] COM(2017) 477 final: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0477:FIN

Orgalime, the European Engineering Industries Association, speaks for 42 trade federations representing the mechanical, electrical, electronic, metalworking & metal articles industries of 23 European countries. The industry employs nearly 11 million people in the EU and in 2016 accounted for some €2,000 billion of output. The industry represents over a quarter of the output of manufactured products and over a third of the manufactured exports of the European Union.

www.orgalime.org

ORGALIME aisbl | BluePoint Brussels | Boulevard A Reyers 80 | B1030 | Brussels | Belgium
Tel: +32 2 206 68 83 | e-mail: secretariat@orgalime.org
Ass. Intern. A.R. 12.7.74 | VAT BE 0414 341 438

international standards could be used as the **primary reference** for the building blocks of future cybersecurity schemes.

Involvement

- ENISA needs a **clear and permanent mandate** in order to improve its efficiency, and to continue help supporting cybersecurity capacity building in the Member States.

- **Industry input** in elaborating and preparing candidate schemes under the new governance structure is limited and **requires improvement**. The Cybersecurity Act needs to elaborate under which conditions ENISA should consult relevant stakeholders, in an open and transparent manner.

- The Cybersecurity Act should take inspiration from Article 18 of the Ecodesign Directive to provide a **pragmatic solution for involving all relevant stakeholders** in the preparation of future compliance and certification schemes, including work plans, quality criteria and a stakeholder consultation forum.

INTRODUCTION

On 13 September 2017, the European Commission presented a series of policy and legislative initiatives aiming at completing and reinforcing the cybersecurity pillar of the Digital Single Market.
It is of critical interest to our industry to provide its customers with increasingly interconnected and smart products and services that are safe and secure. Cybersecurity is a prerequisite for the functioning of the Digital Single Market and a fast moving target, which cannot be solved by one-fits-all solution. Our industry is committed to provide customers with the highest level of protection possible against any cyber-attack or unauthorized harmful manipulation or destruction of data. Orgalime is committed to enhancing Europe’s cybersecurity capacity and to nurture trust in ICT products and services. The Commission proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'') is a first step towards a safer and more secure European Digital Single Market.

However, we are concerned that the current draft proposal for a regulation and the regulatory format of a European Cybersecurity Certification Framework (ECCF) fundamentally depart from the robust experience of European harmonisation legislation for products introduced by the New Approach to technical harmonisation and codified in a “New Legislative Framework” (NLF) in 2008. Orgalime underlines the importance and relevance of NLF principles when it comes to legislation applying to the placing of products on the market. These are based on international and European standards, flexible adaptation of product requirements via standardisation procedures, well-established and widely accepted conformity assessments procedures (including the manufacturer’s self-declaration of conformity and third party certification). Such a well-established system strives for broad acceptance by users and providers, safeguarding a level-playing field within the market for domestic manufacturers and importers, and finally an adequate and effective enforcement.

Finally, static schemes do not necessarily offer the preferred approach to cybersecurity. Therefore, a sectoral approach that takes into consideration the different exposure levels, threats and security architectures of individual economic sectors is necessary as a one-size-fits-all approach will not be appropriate to promote cybersecurity.

1. THE SCOPE AND DEFINITION OF THE ACT SHOULD FOCUS ON ICT PRODUCTS AND SERVICES INTERCONNECTED WITH THE INTERNET

Orgalime is representing all manufacturers of industrial automation and products and systems that are supplied to consumers or other end-users. Many of these products belong to the industrial automation sector with accompanying services. Examples of products incorporating ICT components range from connected doors, building or industrial hardware, smart valves, connectors, sensors of all types, to industrial or commercial robots, collaborative and autonomous robots and systems, smart devices for unmanned crafts (drones) etc.

As such, Orgalime represents the whole range from Industrial Automation and Control Systems (IACS), products and solutions that integrate these IACS, to consumer products in a very large variety of customer markets.

For our industry it is crucial to provide products and solutions to our customers that are state-of-the art cyber-secure, both on the professional markets (B2B) and consumer markets (B2C). In both cases we believe that the definition of "***ICT product and services***" meaning "*any element or group of elements of network and information systems*" should clarify that these are likely to be physically or wirelessly **interconnected with the Internet**, whether intentionally or not. Further clarification is needed to define the scope of services to be covered under the certification scheme as they vary from physical products in terms of their security requirements, operating environment and vulnerability.

2. SELF DECLARATION OF CONFORMITY IS A VALID ALTERNATIVE TO THIRD PARTY CERTIFICATION FOR THE BASIC LEVEL OF CYBERSECURITY

Third-party certification is not always appropriate to promote cybersecurity in the market. By experience, private contracts applying to professional (B2B) products combined with the use of standards and alternative conformity assessment procedures often provide more adequate, cost-efficient and flexible answers to manufacturers, especially SMEs.

Because future cybersecurity schemes may to some extent become by law or in practice mandatory, Orgalime calls on the co-legislators to consider other conformity assessment procedures such as self-declaration of conformity as a viable alternative to third-party certification only. Cybersecurity is a "moving target" and each certification scheme reflects a certain testing and compliance procedure to particular requirements at a certain point in time. Certification and possible re-certification by third-parties is time and cost intensive, especially for SMEs, and may delay time-to-market. The option of self-declaration of conformity combined with effective and efficient market surveillance mechanisms gives manufacturers more flexibility, fosters innovation, and leverages the level of cybersecurity. This is also reflected by basic principles coming from the New Approach to technical harmonisation and the New Legislative Framework for the making available of products on the EU Internal Market.

In particular, such an option could apply to the first "basic" level of cybersecurity, depending on the category of ICT products and their intended use-case applications. As many of these ICT products are already covered by Union harmonisation legislation to address aspects of health and safety where such flexibility already exists, it would be illogical and detrimental to economic operators to prevent them from benefitting from the same level of flexibility in assessing the resilience of their ICT products to cyber-attacks.

In 2014, the European Commission (DG CONNECT) and the JRC have already dedicated some thoughts to the issue by sponsoring the thematic group on the European IACS Cybersecurity Certification Framework (ICCF), which provides for such a module of self-declaration of conformity: "*The vendor hereby declares that they positively assessed this product against the IACS Common*

Cybersecurity Assessment Requirements selected in a Security Profile that can be consulted online on the IACS C&C EU Register” [2].

3. CYBERSECURITY BY DESIGN SHOULD BE INCLUDED IN A RISK-BASED APPROACH

Orgalime welcomes the Commission's ambition to promote the take up of cybersecurity good practices in all human activities, beyond those already applied in sensitive civil and military infrastructures.

To that end, **cybersecurity-by-design** is a concept that may be recommendable to ICT components, whereby claims need to be sustained by applying a conformity assessment procedure based on clear and verifiable technical requirements and processes. However, this useful concept could be complemented to build trust in the market. Although connected products embed certified components, this does not always guarantee protection or cyber security.

Therefore, Orgalime recommends using a **risk-based approach** to determine which requirements, procedures and schemes should be prepared as a priority, taking duly into consideration cybersecurity-by-design altogether with the **cybersecurity "ecosystems"**: it is in our view necessary to assess cybersecurity vulnerabilities by taking ICT components, products and systems as well as their risk environment, overall operation and management procedures into account.

4. THE VOLUNTARY NATURE OF CERTIFICATION SCHEMES IS A PRIORITY

We understand the Commission intention is to stimulate good cybersecurity practices among the many industry sectors that will be involved in the placing of ICT products on the market. Therefore, Orgalime principally welcomes the **voluntary nature** of the future certification schemes (Article 48(2)). However a cybersecurity scheme for certain categories of products could "*de jure*" become mandatory through binding references to other EU legislation, as provided for in Article 48 of the draft proposal.

Moreover, we are concerned that depending on the structure of the market where the categories of ICT products and services are expected to be placed and used, future cybersecurity schemes may become "*de facto"* mandatory for the manufacturers or distributors of such products.

This may be the case as a result of the market power of major economic operators and could very likely lead to the detriment of small/medium size manufacturers of ICT components and sub-systems versus their much larger customers-integrators of such ICT components and sub-systems. In addition to that, mandatory schemes can occur as a result of public procurement practices that often require a number of non-legally required certifications for the procured products.

This is why we consider that future cybersecurity compliance and certification schemes should be carefully prepared based on expected consequences coming from market dynamics, product development, risk environment and implications of the legal framework conditions. The best approach would be to prepare them along the predefined model of the New Legislative Framework (including conformity assessment modules A to H as described in Decision 768/2008 EC).

5. EUROPEAN AND INTERNATIONAL STANDARDS ARE A KEY REFERENCE

The industry represented by Orgalime is especially familiar with European harmonised standards as defined in Regulation (EU) 1025/2012. Their use grants them a presumption of conformity with EU

[2] https://erncip-project.jrc.ec.europa.eu/sites/default/files/2015_1441_src_en_pth-erncip-iacsreport-201411-at-accepted_pth2-op.pdf

"essential requirements" set in the law, mostly for the purpose of protecting core EU interests in health and safety, the environment, energy and natural resources. As international standards can open doors to global trade, European standards should take into consideration international standards as a main point of reference.

Yet it is disappointing to see that the Cybersecurity Act makes no commitment to international standards. The role of the international dimension of standardisation is core to the competitiveness of our industry. In the electro-technical field alone, 80% of European standards are equal to international IEC standards, which provides European-based industries a clear advantage to access world markets. This advantage exists for 40% for machinery standards (increasing), which provides a highly significant benefit for our industry.

The European Cybersecurity Certification Framework should set out in a clearer way where standards should be used for cybersecurity requirements. European and international (ISO/IEC,) standards should be used to provide independent, objective validation of the reliability, quality and trustworthiness of ICT products tailored to the sector-specific needs of the multi-fold variety of industry sectors. Such common criteria help setting specific information assurance goals including strict levels of integrity, confidentiality and availability for systems and data, accountability at the individual level, and assurance that all goals are met.

Orgalime calls on the co-legislators to be more specific as to the possibility of future cybersecurity compliance and certification schemes to refer to existing and future European harmonised standards for defining cybersecurity requirements, common criteria. In this context, international standards and international cybersecurity certification schemes (one is under development in IEC) should be taken into consideration and used as a starting point to define requirements and categories of ICT products and services under the ECCF.

6. THE ROLE AND GOVERNANCE OF ENISA SHOULD BE CLARIFIED

Orgalime underlines the importance to have a clear and permanent mandate of ENISA that clearly defines distribution of competences between national authorities and ENISA in order for ENISA to fulfil their task even better, by improving efficiency and avoiding unnecessary parallel structures. This is particularly needed to get synergies between authorities at national and EU level, for instance the coordination and assistance to prevent and detect major cyber incidents, the collection and dissemination of information to public and private stakeholders about best practices, capacity building and prevention strategies. Such a tool may especially be helpful for SMEs that do not have the resources to run a large IT department and smaller Member States with resource restricted Computer Security Incidence Response Teams (CSIRTs).

The proposed regulation intends to give ENISA the role of a facilitating body in order to prepare future cybersecurity certification schemes. Orgalime seriously doubts that the preparation and deployment of complex certification schemes alongside many other abovementioned responsibilities could be properly, efficiently managed by ENISA alone in a timely manner, in addition to its primary role which is to assist European Member States in cybersecurity matters. The creation of EU-wide certification schemes calls for simple but well-functioning, transparent and inclusive governance structures with the participation of representatives from private and public sector. Every single scheme should be able to cope with market dynamics, technological developments, a suddenly changing risk environment and international standards.

7. ALL STAKEHOLDERS SHOULD BE INVOLVED IN SHAPING FUTURE CYBERSECURITY CONFORMITY AND CERTIFICATION SCHEMES

The cybersecurity of an ICT product or service depends inherently on the overall result of the cybersecurity assessment of the product or service under consideration. This involves considerations for several aspects that require expertise from a variety of stakeholders to conduct a cybersecurity development lifecycle, an assessment of the functional security of the product, its components and the system in which these are incorporated.

Article 44 paragraph 2 envisages that "(…) *ENISA shall consult all relevant stakeholders*". In the light of our previous considerations, we believe that this is not enough and needs to be improved: To be successful in defining cybersecurity requirements, security levels and procedures for implementing secure interconnected ICT products and services, we believe that ENISA should involve at least following categories of business stakeholders:

- **manufacturers** responsible for assessing the risk, designing, manufacturing, implementing, or managing IoT devices and systems,
- **cybersecurity solution providers,**
- **system integrators**, security practitioners, maintenance specialists and
- **end-users** (i.e. asset owner) of the resulting ICT products and services.

→ See our concrete suggestions in Annex 1

8. THE CONSULTATION PROCESS FOR PREPARING FUTURE CYBERSECURITY COMPLIANCE AND CERTIFICATION SCHEMES SHOULD BE MORE DETAILED AND TRANSPARENT

As explained above, the preparation of future cybersecurity compliance and certification schemes should rely on the involvement of a variety of stakeholders that are knowledgeable about conducting a cybersecurity development lifecycle of the product or system under consideration. To handle such complexity in full transparency, Orgalime recommends using a similar approach as the one described in the Ecodesign Directive 2009/125/EC Article 18 for a structured and efficient consultation process, which consider alike the expertise and **"*balanced participation*" of all relevant stakeholders in a "Consultation Forum"** to assessing the necessary requirements and procedures that shall apply to the product for the purpose of the EU legislation.
→ See our concrete suggestion in Annex 1

9. NATIONAL CERTIFICATION SUPERVISORY AUTHORITY SHOULD BE GRANTED MORE POWERS TO ENFORCE THE VOLUNTARY APPLICATION OF THE SCHEMES BY THE MARKET

The take-up of good practices via the deployment across a business sector of a cybersecurity certification scheme depends significantly on the ability of Member States to enforce such a scheme. Confidence and trust in ICT products and services is key for end-users and consumers in the Single Market. Therefore the implementation and enforcement of ECCS should go hand in hand with adequate, effective and transparent market surveillance. The establishment of a "*national certification supervisory authority*" in each Member State as part of the European Cybersecurity Certification Group is thus indispensable (Draft Regulation, Article 50).

In practice, it is likely that all types or categories of ICT products or services are already/ will be subject to essential safety and other core-EU requirements under legislation pertaining to these categories of products or service. Therefore, we believe that the draft EC proposal should ensure that the planned "*investigations, in the form of audits, of conformity assessment bodies and European cybersecurity certificates' holders*" should be coordinated within the overall framework on the enforcement of Union harmonisation legislation on products under Regulation EC 765/2008 or any upcoming revision of that framework (see COM(2017) 795 final).

Responsible advisers: Philippe Portalier & Gerrit Steinfort
(firstname [dot] lastname @ Orgalime.org)

Annex 1 – Concrete suggestions to improve the framework for the preparation of European cybersecurity compliance and certification schemes

Open and transparent stakeholder consultation process

Therefore, Orgalime suggest taking up key steps of the stakeholder consultation process as described in the Ecodesign Directive 2009/125/EC of 21 October 2009 and in particular:

1. The requirements for each type or categories of ICT products or services shall be formulated so as to ensure that national certification supervisory authorities can verify the conformity of the product with the requirements of the cybersecurity compliance and certification schemes. The scheme shall specify whether verification can be achieved directly on the product or on the basis of the technical documentation (similar formulation as in Directive 2009/125/EC Article 15(7)).
2. ENISA shall ensure participation of Member States' representatives and all important parties concerned with the ICT product group or service in question. This includes industry along value chains, (, trade unions, traders, retailers, importers, conformity assessment bodies and end-consumers. These parties shall contribute to defining and reviewing cybersecurity schemes, to examining the effectiveness of the established enforcement mechanisms set out in Article 50§6 and to assessing the application of the scheme. These parties shall meet regularly in a Consultation Forum. The rules of procedure of the Forum shall be established by the Commission (similar formulation as in Directive 2009/125/EC Article 18).

Self-declaration of conformity and use of harmonised standards

Similarly, we believe that the European Cybersecurity Certification Framework should better integrate and underline self-declaration of conformity assessment procedure, for the basic level of cybersecurity assurance. Such conformity assessment procedure should make a clear reference to the use of European and international harmonised standards. Consequently, the proposal of a Cybersecurity Act should provide for that option under Title III of this Regulation:

1. For the basic level of cybersecurity, the conformity assessment procedures shall be specified by the Cybersecurity Product Scheme and shall leave to manufacturers the choice between the internal design control set out in Annex […] to this Regulation and third-party certification set out in Article 48 of this Regulation. Where duly justified and proportionate to the risk, the conformity assessment procedure shall be specified among relevant modules as described in Annex II to Decision No 768/2008/EC (similar formulation as in Directive 2009/125/EC Article 8(2) sub2).
2. If a product or service covered by a cybersecurity scheme includes the product or service design function and which is implemented in accordance with harmonised standards, the reference numbers of which have been published in the Official Journal of the European Union, that cybersecurity product or service shall be presumed to comply with the corresponding cybersecurity requirements set out in the cybersecurity scheme (similar formulation as in Directive 2009/125/EC Article 8(2) sub 4)

Governance criteria for the preparation of ECCS

It is necessary to provide clear, inclusive and transparent governance criteria to equally involve needed input by Member States, the European Commission, ENISA and affected stakeholders to prepare European Cybersecurity Certification Schemes (ECCS) in order to provide credibility, trust and broad acceptance of ICT products and services within the Single Market. In that respect, we recommend future ECCS to be assessed against the following criteria (similar to those set out in Directive 2009/125/EC on Ecodesign, Article 15):

1. In view of mandating ENISA for the preparation of a draft ECCS, the Commission shall

take into account any views expressed by the Committee referred to in Article 19(1) and shall further take into account:

(a) Community cybersecurity priorities, such as those set out in Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union; and

(b) relevant Community legislation and self-regulation, which are expected to achieve the policy objectives more quickly or at lesser expense than cybersecurity certification requirements.

2. In preparing a draft ECCS, ENISA shall:

(a) consider the life cycle of the ICT product or service and all its significant connectivity aspects, inter alia to the Internet. The depth of analysis of the connectivity aspects and of the feasibility of their resilience to cyber-attacks shall be proportionate to their significance. The adoption of requirements on the significant cybersecurity aspects of a product or service shall not be unduly delayed by uncertainties regarding the other aspects;

(b) carry out an assessment, which shall consider the impact on the environment, consumers and manufacturers, including SMEs, in terms of competitiveness – including in relation to markets outside the Community – innovation, market access and costs and benefits;

(c) take into account existing national legislation on cybersecurity that Member States consider relevant;

(d) carry out appropriate consultation with stakeholders; and

(e) prepare an explanatory memorandum of the draft cybersecurity requirements based on the assessment referred to in point (b)

3. In preparing a draft ECCS, ENISA shall meet all the following criteria, bearing in mind that cybersecurity requirements and compliance schemes may become mandatory as set out in Article 1(b) and 48(2):

(a) there shall be no unjustified negative impact on the functionality of the product, from the perspective of the user;

(b) health, safety and the environment shall not be adversely affected;

(c) there shall be no significant negative impact on consumers in particular as regards the affordability of the product;

(d) there shall be no significant negative impact on industry's competitiveness inside and outside of the Single Market;

(e) in principle, the setting of cybersecurity requirements and assurance levels shall not have the consequence of imposing proprietary technology on manufacturers; and

(f) avoiding administrative burden on manufacturers.

4. The requirements shall be formulated so that market surveillance authorities can verify the conformity of the product with the requirements of the ECCS in a manageable and timely manner. The ECCS shall specify whether verification can be achieved directly on the product or on the basis of the technical documentation.

Annex 2 – Glossary of terms used in this position paper:

B2B: Business-to-business, designating a relationship among knowledgeable professionals usually governed by private contracts.

B2C: Business-to-consumers, designating a relationship between an economic operator (manufacturer or distributor) usually governed by private contracts.

CSIRTs: Computer Security Incidence Response Teams as referred to in Article 6 of the EC COM(2017) 477 final.

ECCS: European Cybersecurity Certification Schemes, as described under Article 43 of the EC COM(2017) 477 final.

ECCF: European Cybersecurity Certification Framework as per Article 1 of the EC COM(2017) 477 final

IACS: Industrial Automation and Control Systems, as codified in the international standard ISA-62443 see the explanatory memorandum of the EC COM(2017) 477 final.

ICCF: IACS Cybersecurity Certification Framework.

ICT: Information and communications technology.

IoT: Internet of Things.

ISA: The International Society of Automation (www.isa.org) is a non-profit professional association that sets the standard for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure.

ISO: International Standards Organisation.

IEC: International Electrotechnical Commission

NLF: New Legislative Framework = Decision 768/2008/EC and Regulation (EC) 765/2008

JRC: Joint Research Center of the European Union.

NIS: Network and Information Systems

SME: Small and Medium-sized Enterprise