ZVEI:
Die Elektroindustrie

Statement

Comments by the electrical industry on the EU Cybersecurity Act

January 2018

German Electrical and Electronic Manufacturers' Association

Summary

This document provides insights of the German Electrical and Electronic Manufacturers' Association and its 1,600 member companies on the draft EU Cybersecurity Act published in September 2017. Advice is given on the further constructive development of the draft regulation currently discussed by the Council of Ministers, the European Parliament and the EU Commission. It is important to ensure that the regulation is implemented in a way that is suitable for industry and promotes innovation in the same time. It is crucial for the ZVEI member companies that:

- priority is given to international harmonised standards;
- industry participation and manufactures' ownership are strengthened;
- third party certification cannot serve as a substitute for trust;
- the design of a „conformity and certification" framework will be developed further;
- mandates regarding necessity and scope for „conformity and certification" schemes are based on clear, comprehensible criteria.

Further key points

Cybersecurity Act raises tensions with the existing EU legal system: With the New Legislative Framework (NLF), the Commission has established a universal and well-established system for the regulation of products and their placement on the EU market. The Cybersecurity Act incomprehensibly re-engineers product requirements and market surveillance regulations in an entirely separate and incompatible way.

Taking WTO aspects into consideration: It would run counter to the objectives of the WTO-TBT agreement if an EU certification scheme were to become a de facto market access requirement in spite of its voluntary nature, without having to be based on international standards and conformity assessment schemes.

Harmonisation with no third-party obligations: The EU Commission's objective in drafting a „Cybersecurity Act" to create uniform regulations for cybersecurity across Europe is both valid and important. The electrical industry expressly welcomes the intention to counteract fragmented certification schemes based on the principle of „one certification, EU-wide recognition". These measures strengthen the European (digital) internal market and contribute to the free flows of data and goods. However, this concern should not be used to de facto mandatorily extend third-party certification to all product and market sectors as a substitute for trust.

Priority of the New Legislative Framework: The Cybersecurity Act will set requirements for products via a certification scheme (see Part 3, Article 47). By referring to products, the Act affects the area of product regulation - without taking into account the previously agreed and established procedures of the European market regulation. The reasoning that the underlying framework is a voluntary instrument in itself cannot, from the electrical industry's point of view, be a basis for disregarding the principles and procedures of the New Legislative Framework (NLF). If requirements are to be placed on products in a direct or indirect form, the ZVEI considers this to be done primarily within the framework of the NLF and based on a risk assessment approach. To ensure an appropriate level of security against cyber-attacks under the New Legislative Framework (NLF), the respective legislation needs to be amended with concrete requirements. Such an approach ensures the following key principles:

- Observance of international norms and standards
- Flexible adapting of requirements via standardisation
- Flexibility for horizontal and vertical requirements
- Established and accepted conformity assessment system
- High acceptance by providers and users
- Ensuring a level playing field for manufacturers and importers
- Regulated procedures and competencies for market surveillance authorities

The danger of cross-references and double regulation: The electrical industry believes there is a risk of serious complications. According to Art. 48 (2), other EU regulations may refer to individual, originally voluntary certification systems that were created within the new framework and thus render them binding. This would instantly give the systems a product regulatory status, even though these systems were not designed according to NLF procedures. This concern is corroborated by current considerations to introduce delegated legal acts with product requirements for cybersecurity under the Radio Equipment Directive 2014/53/EU (RED) Art. 3 (3). If product regulation for security is required, this should be done based on a comprehensive risk assessment and in accordance with the principles of the NLF. This provides all the essential tools and procedures, including conformity assessment and monitoring in the marketplace and, where applicable, the possibility of third party certification.

Inadequate industrial participation: The Cybersecurity Act needs a firm and lasting inclusion of market and customer insight as well as technical expertise about product development from companies in the application and manufacturing sectors. Otherwise, there is an imminent risk that the certification schemes may be in conflict with key customer and market requirements. This would be likely to result in the failure of the EU framework. The current reference to industrial participation (Title 3, Article 44 (2)) is insufficient. The Eco-Design Directive (2009/125/EC) provides a good template for a structured and effective process of consultation.

Clear assessment criteria for initiation: On the basis of Art. 44 (1) of the Cybersecurity Act, it is not clear in any way what criteria should be used to determine the need for, requirements and scope of a new certification schemes. Based on a catalogue of criteria, the checklist procedure should be used by the Commission to examine potential existing schemes, as well as the need for, the benefits and the foreseeable consequences of a new scheme. The criteria have to be worked on together with the industry in order to be able to depict general conditions such as market dynamics, technological developments, risk changes and international standardisation and norms. Only when the criteria have been assessed positively should the question of whether a new European certification system is applicable and its scope be determined. The Commission's current sweeping right of initiative under Article 44 (1) is insufficient from the electrical industry's point of view.

Process-related separation of content from conformity assessment: The Cybersecurity Act combines the determination of

- the levels of trustworthiness and testing depth (Art. 46),
- the contextual requirements and elements (Art. 47) as well as
- the type of conformity assessment (Article 48, solely by means of certification)

into one process. This creates a mixture of mutually independent parameters. The determination of appropriate conformity assessment procedures (from manufacturer's self-

declaration to third party certification) only makes sense when the scope of application, protection objectives, risk enviroment, as well as customers' and market requirements have been clarified (own responsibility of the manufacturer's declaration of conformity or certification by a third party). The definition of the „what" (Art. 45 - 47) should therefore be separated from the assessment of the „how" (Art. 48 in an adapted form) in a procedural manner and determined in close coordination with all relevant stakeholders.

Name modification: The existing naming of the elements of the European certification framework already necessitates a commitment to third-party certification. As described above, the framework should also include the established and proven possibilities of conformity assessment as defined and available in NLF Decision 768/2008/EC with Modules A to H. The necessary additions to the content should be reflected in the naming. Therefore, the ZVEI is suggesting a change in the name:

- Conformity and Certification Framework
- Conformity and Certification Scheme
- Conformity and Certification Group

Strengthening manufacturers' ownership: Certified products and applications are not necessarily more secure or trustworthy than non-certified products. A certification corresponds to a test made according to pre-defined rules and requirements at a specific time. This means that dynamic changes in the cybersecurity environment and parameters not provided for in the test procedures cannot be detected by a certification of a prototype. On the other hand, the manufacturer self-declaration procedure enables a prompt and flexible reaction to changing conditions and can also provide the relevant information on cybersecurity. When combined with strong market surveillance, it ensures the provision of binding, reliable and legally effective information. It can therefore achieve at least the same degree of transparency and trust as certification but above all fulfilment of technical requirements -for the end customer. By basing their evaluation and manufacturer's declaration on a risk based approach, companies can define the appropriate protection level – for the entire product life cycle. Not every product has to be protected with high security. Of course, wherever life or health depends on the products and solutions, there certainly must be other requirements than, for example, in the consumer goods sector. Here, third-party-certification can be useful – if not already in place.

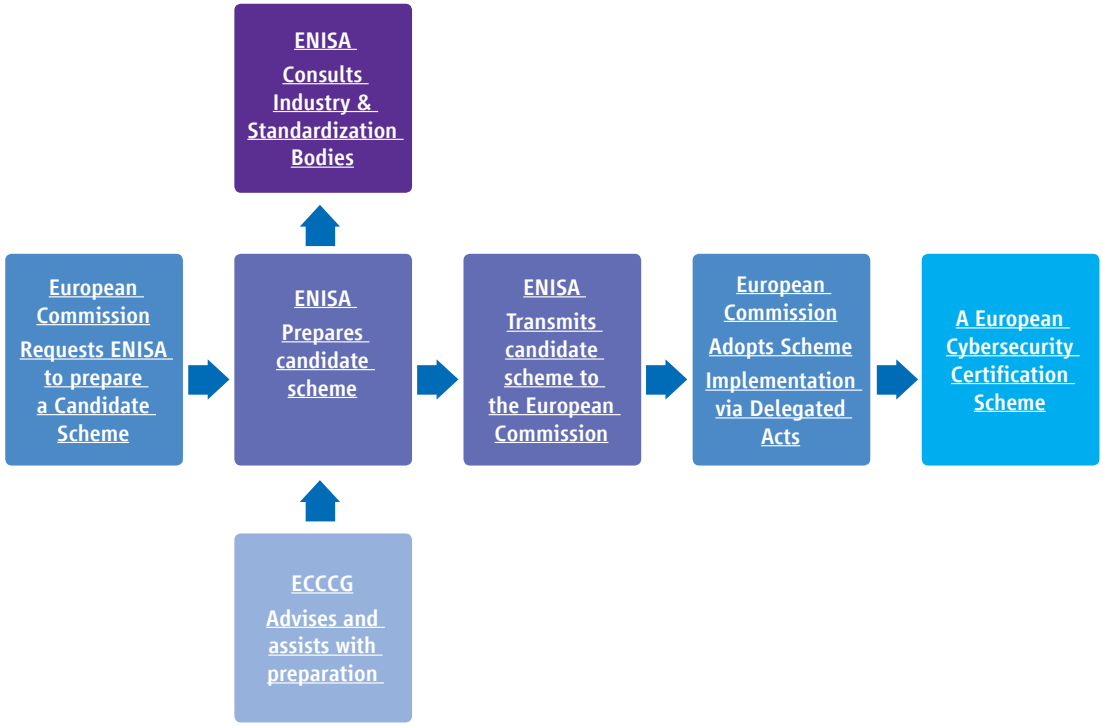
Strengthening market surveillance: Experience has shown that any system (whether voluntary, harmonised or regulated) without strong market surveillance cannot succeed. Market surveillance creates a level playing field and ensures the reliability of the information provided on the market (e. g. manufacturer's declarations). To ensure effective evaluation of cybersecurity of products, market surveillance authorities need significantly more resources, meaning more budget and staff. Evaluating cybersecurity requires comprehensive and deep knowledge as well as effective testing procedures. Member states need to make sure that effective market surveillance procedure are established. Unlike the NLF, the Cybersecurity Act does not currently provide a strong role for market surveillance and relies primarily on the activities of the conformity assessment bodies as third parties. In most cases, however, it will only be able to take appropriate action against misuse and violations of the law in a limited or even ineffective manner.

Taking the different user competences into consideration: In general, no security knowledge can be assumed in private end users. In industrial environments, operators and users bear defined responsibilities and possess the necessary expertise. This fact should be taken more into account by the Cybersecurity Act when selecting and designing a certification system.

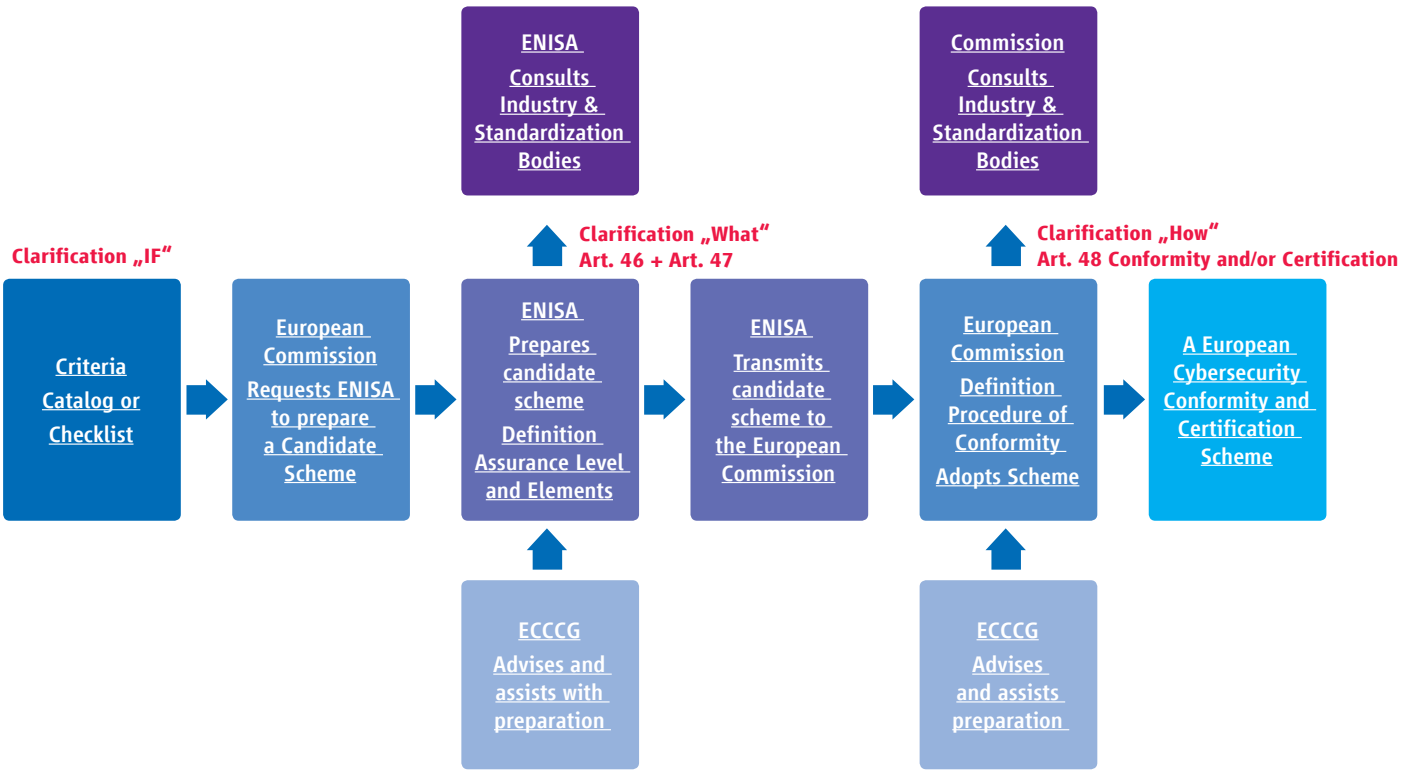
Reviewing flexibility: With the ever-changing implications for security and the wide range of options available to meet them, product certification is approaching its limits. If this occurs, the certification of a system appears to be preferable (see Quality Management).

Adaptation of the process model

Existing process model in draft for the Cybersecurity Framework:



Proposal for an adapted process model:



Recommendations on how to adapt the text

Basis: *"Proposal for a Regulation of the European Parliament and of the Council on ENISA, the EU Cybersecurity Agency (Cybersecurity Act)"* from 13.9.2017 (COM(2017) 477 final)

Notice: The following table only contains amendments for the implementation of the ZVEI core requirements. In terms of the consistency and plausibility of the text, this results in continuous changes to the entire documents, which are not listed here separately. The entire text must always be checked for consistency with the proposed text adaptations and modified if necessary.

Section	Current text wording	Recommendation
Art. 43	A European cybersecurity certification scheme shall attest that the ICT products and services that have been certified in accordance with such scheme comply with specified requirements as regards their ability to resist at a given level of assurance, actions that aim to compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, processes, services and systems	A European cybersecurity conformity and certification scheme shall attest that the ICT development and maintenance processes that have been certified in accordance with such scheme comply with specified requirements as regards their ability to resist at a given level of assurance, actions that aim to compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, processes, services and systems
Revised Art. 44 (1)		The Commission proves the necessity, relevance, usefulness, scope, and impact of a possible scheme based on commonly agreed on criteria. Possible criteria are: if all the following criteria are fulfilled: a) There is a relevant information gap between the provider and the buyer of the product or service. b) The information gap cannot be remedied by agreements and voluntary actions of the private market players. c) The candidate European cybersecurity attestation scheme is suitable to remedy the information gap.
Art. 44 (1)	Following a request from the Commission, ENISA shall prepare a candidate European cybersecurity certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this Regulation. Member States or the European Cybersecurity Certification Group (the 'Group') established under Article 53 may propose the preparation of a candidate European cybersecurity certification scheme to the Commission.	After a positive evaluation of the criteria, the Commission issues a request to ENISA. Following the request from the Commission, ENISA shall prepare a candidate European cybersecurity conformity and certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this Regulation. Member States or the European Cybersecurity Conformity and Certification Group (the ‚Group') established under Article 53 may propose the preparation of a candidate European cybersecurity Conformity and Certification scheme to the Commission.

Art. 44 (2)	When preparing candidate schemes referred to in paragraph 1 of this Article, ENISA shall consult all relevant stakeholders and closely cooperate with the Group. The Group shall provide ENISA with the assistance and expert advice required by ENISA in relation to the preparation of the candidate scheme, including by providing opinions where necessary.	When preparing candidate schemes referred to in paragraph 1 of this Article, ENISA shall define the security objectives (see Art. 45), assurance levels (see Art. 46), and elements (see Art. 47) of the candidate scheme. All aspects regarding the procedures of the conformity assessment will be defined by the Commission in a second step, based on ENISA's findings. In doing so, ENISA shall work closely together with the industry stakeholder group and consult all relevant stakeholders and closely cooperate with the Group. The Group shall provide ENISA with the assistance and expert advice required by ENISA in relation to the preparation of the candidate scheme, including by providing opinions where necessary.
Art. 44 (4)	The Commission, based on the candidate scheme proposed by ENISA, may adopt implementing acts, in accordance with Article 55(1), providing for European cybersecurity certification schemes for ICT products and services meeting the requirements of Articles 45, 46 and 47 of this Regulation.	The Commission, based on the candidate scheme proposed by ENISA, may adopt implementing acts, in accordance with Article 5 of Regulation (EU) No 182/2011, providing for European cybersecurity conformity and certification schemes for ICT products and services meeting the requirements of Articles 45, 46 and 47 of this Regulation. The implementing acts shall contain information based on the council decision (768/2008/EC) about what type of conformity assessment should be chosen for the scheme. The type of conformity assessment shall be chosen in accordance with the criteria given in Article 4 of Council Decision 768/2008/EC.
Art. 47 (b)	detailed specification of the cybersecurity requirements against which the specific ICT products and services are evaluated, for example by reference to Union or international standards or technical specifications;	detailed specification of the cybersecurity requirements against which the specific ICT development and maintenance processes are evaluated, for example by reference to Union or international standards or technical specifications. In relation to the technical requirements and evaluation procedures, the schemes shall , whenever possible, make use of existing standards and shall not develop the technical standards themselves. Note: In the case of referencing European standards, these are published by the European standardisation organisations and endorsed by the European Commission by publication in the Official Journal (see Regulation 1025/2012).
Art. 47 (c)	where applicable, one or more assurance levels	where applicable, one or more assurance levels and type of conformity assessment
Art. 47 (d)	specific evaluation criteria and methods used, including types of evaluation, in order to demonstrate that the specific objectives referred to in Article 45 are achieved;	specific evaluation criteria and methods used, including types of evaluation, in order to demonstrate that the specific objectives referred to in Article 45 are achieved. Whenever possible for criteria and methods, the schemes shall make use of existing standards and shall not develop the criteria and methods themselves.
Art. 48 (3)	A European cybersecurity certificate pursuant to this Article shall be issued by the conformity assessment bodies referred to in Article 51 on the basis of criteria included in the European cybersecurity certification scheme, adopted pursuant to Article 44.	A European cybersecurity conformity and certification certificate pursuant to this Article shall be issued by the bodies referred to in Article 51 on the basis of criteria included in the European cybersecurity conformity and certification scheme, adopted pursuant to Article 44.

ZVEI:
Die Elektroindustrie

Comments by the electrical industry on the EU Cybersecurity Act

German Electrical and Electronic Manufacturers' Association
Lyoner Strasse 9
60528 Frankfurt am Main, Germany

Contact: Lukas Linke
Phone: +49 69 6302-432
E-mail: linke@zvei.org

January 2018

www.zvei.org