Policy statement

5 October 2018

Strengthening Europe's cyber resilience

Recommendations for trilogue negotiations on the EU Cybersecurity Act

A market-driven approach

Security certification is a well-established global practice to enhance the security of products and services. We welcome the objective of the EU Cybersecurity Act to reduce fragmentation by applying EU sector-specific security certification schemes.

It is in industry's best interests to incorporate the highest possible levels of security in products and services, 'baked-in' through security by design and assured through stringent security standards, such as the ISO 27000 series.

In defining the framework for future EU certificates, we call upon the EU institutions to take into account existing international standards and practices adopted by industry. Industry should keep the ability to define the best suitable tools to achieve a given security objective. We therefore believe that any EU certification scheme should remain voluntary.

A strong industry involvement

A close partnership between European Union Agency for Network and Information Security (ENISA) and industry is critical to achieve higher levels of cybersecurity. The private sector is well-positioned and already encouraged today to both secure its own technologies and share best practices. As its responsibilities increase, ENISA should step up its stakeholder engagement through a formal, open, transparent and inclusive consultation process with industry. The preparation of the certification candidate scheme should be accompanied by engagement with industry and other key stakeholders at all stages of the process thanks to permanent structures. Therefore:

- We support **Amendments 29, 124, 129, 130** as adopted by the European Parliament reinforcing cooperation between ENISA and key stakeholders.
- We support **Amendments 152 and 165** adopted by the European Parliament creating a permanent Stakeholder Certification Group and ad-hoc committees.

The stakeholder certification group should be distinguished from the already existing ENISA Permanent Stakeholder Group, as it will be focusing on ENISA's competences within Title III. In this context, ENISA should be permitted to propose to the Commission the preparation of a candidate scheme.

Specific ad-hoc committees for each proposed scheme involving industry are necessary to gather the required expertise relating to specific schemes. We also recommend that such committees remain in place after the schemes have been adopted to allow for them to be maintained and revised, as well as to monitor developments in the given sector.

A risk-based approach

We welcome the efforts reflected in the positions adopted by the Council and the European Parliament to include a risk-based approach in the application of assurance levels. Assurance levels (if applicable) for a given scheme should be linked to the actual testing and assessment of the product, service or process rather than 'the intended use', which could impede smaller companies to certify their technology. Furthermore, defining assurance levels without taking into account the risk will be too static considering the diversity of risk situations.

We welcome the recognition of the possibility to use self-assessment of conformity. However, it is currently unnecessarily prescriptive and restrictive to limit this practice to the basic level of assurance if adequate internal safeguards are in place in addition to the growing reliance on self-certification in key areas such as encryption. Moreover, the substantial level of assurance potentially includes a wide category of products, services and processes. Therefore:

- We support **article 46 as proposed in the Council General Approach** clearly linking assurance levels to assessment requirements.
- We are concerned by **Article 47a** in the Council position and **Amendments 39 and 183** adopted by the European Parliament limiting self-assessment of conformity to the category falling under a basic level of assurance.

Consistent security requirements

We welcome the efforts reflected in the positions adopted by the Council and the European Parliament to clarify the elements to be defined by a scheme on a case-by-case approach. However, we are concerned that some additional requirements introduced are not consistent with security practices. In particular:

- We are concerned by **Amendment 198** adopted by the European Parliament on not-publicly known cybersecurity vulnerabilities disclosure procedures after they have been detected

Industry follows a disclosure practice called Coordinated Vulnerability Disclosure (CVD), under which a cybersecurity vulnerability is publicly disclosed only after mitigations are deployed. This protects technology users because public disclosure before mitigations are found could allow cybercriminals to exploit the vulnerability. European cybersecurity certification schemes should refer to international standards and best practices on CVD that have been developed by standardisation organisations and multi-stakeholder fora such as ISO, FIRST, ICASI and are already broadly deployed by industry across sectors.

- We are concerned by **Amendment 202** (on Article 47a) proposed by the European Parliament introducing an obligation to issue a document on cybersecurity information.

There is a strong market incentive to inform the user of the security of its product and therefore the requirement to introduce a document on cybersecurity information is unnecessarily prescriptive. Moreover, this requirement is in contradiction with the voluntary certification of ICT products, services and processes. Finally, such a document does not increase the cyber resilience of a product, service or process and only risks creating a false sense of security for the consumer.

Transparent implementation

Last but not least, in order to ensure transparency and stakeholder consultation in the implementation of the framework, we support the approach for adopting certification schemes and related elements by delegated acts (as proposed in **Amendments 51, 54, 57, 69, 162, 167** by the European Parliament), in particular for the adoption of schemes.

We trust that these points will be considered for the ongoing negotiations, which we hope will lead to an effective cybersecurity certification framework in Europe.