THE EU CYBERSECURITY AGENCY

GETTING DOWN TO BUSINESS: ENISA IN THE EU CYBERSECURITY CERTIFICATION FRAMEWORK

November 2018

ENISA is prepared to engage and support all involved stakeholders and fulfil all assigned tasks and roles.

INTRODUCTION

In an effort to harmonise the current cybersecurity certification activities and policies across the Member States, 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"), COM(2017) 477[1], (hereinafter, the Proposal) establishes, the European Cybersecurity Certification Framework for ICT products and services. This proposed framework seeks to lower financial and administrative barriers for the industry by pursuing the setting up of an EU cybersecurity certification framework for ICT products and services.

This paper presents an outline of the perceived role of ENISA concerning these emerging functions and tasks based on the Proposal. Following the finalization of the legislative procedure and the publication of the Regulation's text in the Official Journal, ENISA is prepared to engage and support all involved stakeholders and fulfil all assigned tasks and roles.

1 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0477

LEGISLATIVE PROVISIONS

With a view to pursue the policy goal of a common framework across the EU, the proposal for the EU Cybersecurity Certification Framework in the draft Cybersecurity Act makes the following provisions for ENISA:

- Lays down an overall framework of rules governing European cybersecurity certification schemes.
- Does not introduce directly operational certification schemes.
- Seeks to create a system (framework) for the establishment of specific certification schemes for specific ICT products/services (the "European cybersecurity certification schemes").
- Provides that certification schemes created in accordance with the Framework will allow certificates issued under those schemes to be valid and recognised across all Member States and to address the current market fragmentation.
- Provides what the minimum content of such schemes should be.

Certification schemes will have to define specific elements setting out the scope and object of the cybersecurity certification such as the identification of the categories of products and services covered. In addition, it is necessary to provide in detail specifications of the cybersecurity requirements (for example by reference to the relevant standards or technical specifications), the specific evaluation criteria and methods and the level of assurance they are intended to ensure (i.e. basic, substantial or high) as they will eventually be specified in legislation.

Certification schemes will have to define specific elements setting out the scope and object of the cybersecurity certification such as the identification of the categories of products and services covered.

GOALS OF ENISA IN THE LEGISLATIVE PERIOD

The primary goal of ENISA throughout the period until the Proposal comes into force is identifying the types of certification schemes that possibly fall within its scope and mandate as per the Proposal. Furthermore, ENISA, as ever, engages with stakeholders with a view to involve them in discussions on the EU cybersecurity certification mandate of the Proposal.

ENISA has been active in analysing prospective schemes based on existing and new application areas (e.g. consumer), classes of products (e.g. IoT) and types of services (e.g. Cloud) in a way that when needed it can quickly respond to requests to draw up candidate certification schemes. Clearly, it is essential for ENISA to continue collecting and validating stakeholder requirements in the area of the EU certification framework as well as make available the necessary organisational conditions required to fulfil its role in a timely manner.

MISSION

The mission of ENISA in the area of the EU cybersecurity certification framework is expected to be defined along the following lines: "To pro-actively contribute to the emerging EU cybersecurity certification framework and carry out the drawing up of candidate certification schemes in line with the Cybersecurity Act, providing stakeholders with a sound service that leads to efficiencies and value in the EU".

Throughout its lifespan ENISA has received due recognition for its outputs. In a shift towards a role that adds more value to the EU policy on network and information security, ENISA has been singled out as the appropriate organisation to deliver on the promise of drawing up candidate certification schemes in an EU cybersecurity certification framework. ENISA with its pivotal role as an interlocutor with both public services as well as the industry and standardisation organisations provides a sound reference point to draw up candidate certification schemes.

The expected output of ENISA pursuant to its envisaged role in the EU cybersecurity certification framework includes draft and finalised candidate schemes for the certification of ICT products and services, in the meaning of the Proposal.

STAKEHOLDERS

Clearly, the success of the role of ENISA depends on support from and cooperation with key stakeholders that include but are not limited to the following ones: the members of the European Cybersecurity Certification Group, including the Commission and competent authorities in the Member States represented thereto. Additionally National Accreditation Bodies, Certification Supervisory Authorities, Conformity Assessment Bodies, European standardisation organisations (CEN/CENELEC and ETSI) as well as international and industry standardisation organisations, product manufacturers and service providers who have an interest in EU schemes for the certification of ICT products and services.

THE ROLE OF ENISA

The role of ENISA at this stage can be determined along the two new competences described in the Proposal, being:

- A role in support of the Commission in relation to the European Cybersecurity Certification Group.
- A role in the drawing up of candidate cybersecurity schemes within the emerging EU framework.

Certification related activities of ENISA is a new policy area for the Agency that aims at making available high quality technical and policy services to its stakeholders. As they will be an integral activity of the Agency, it is expected that relevant operations begin as soon as the Proposal is approved. On the outset, ENISA aims at targeting the drawing up of candidate schemes for the cybersecurity certification of ICT products and services. ENISA seeks to draw up candidate schemes in an array of application areas (e.g. consumer), classes of products (e.g. IoT) and types of services (e.g. Cloud). These candidate schemes are likely to be drawn up with the support of stakeholders, which can be public entities in the Member States and private companies alike, as well as professional groups/associations and individuals.

This approach is likely to give ENISA the flexibility it needs to successfully secure and complete candidate certification schemes integrating various elements and ranges of stakeholders' requirements. By relying on existing schemes, ENISA is likely to tackle the transition into an EU cybersecurity certification framework more rapidly, thus supporting the quick up take of the framework across the EU.

Concurrently, ENISA is also likely to take up initiatives in other areas in need of cybersecurity certification schemes. Clearly, any activation of the capacity that ENISA is likely to build in certification requires a formal Commission request. In the same vein, the Commission is the final recipient of ENISA-churned out candidate certification schemes.

The needs for certification schemes across select Member States has continued to proliferate by means of initiatives of select Member States that have recognised over time the high demand prevailing. It is reasonable to suggest that most Member States do not have the capacity to carry out such activities and as such, do not necessarily nurture the ambition to offer or contribute to this sort of service. Therefore, ENISA seeks to set the stage as a possible reference point for all cybersecurity certification scheme-drawing activities across the EU; this of course includes support for the ambition of Member States that do not currently have this capacity, which however may want to get to this point. This is a role in support of the ambition to bring the value of the EU framework across the Member States but also to support the industry, in their efforts within the Internal Market and beyond.

WORKING PRINCIPLES FOR DRAWING UP SCHEMES

A candidate European cybersecurity certification scheme prepared by ENISA needs to be based on sound principles, encouraging stakeholders to contribute to its development and allowing industry and the Member States to benefit from it once approved. The envisaged principles for ENISA drawing up candidate schemes include the following:

- **Open:** a candidate scheme is drawn up by means of open consultations accessible to all parties interested in the technology, products or services affected by the said scheme. For instance, ENISA can invite area Experts to express their interest in the drawing up of a certification scheme, for example by being involved in a consultation process.
- **Consensus driven:** The consultation process is collaborative and consensus based.
- **Transparent:** Any new scheme activity is publicised broadly through means available to ENISA. Information concerning technical discussions and consultations is recorded. Feedback received during the consultation process is treated in an equitable manner and responses are provided for.

CONCLUSION

With the addition of a competence in the cybersecurity certification of ICT products and services, ENISA seeks to step up its contribution to policy on network and information security in the EU. Clearly, stakeholder involvement is key, much as guidance from EU institutions and EU Member States is. At the end of the day, ENISA has been established as a support measure in the internal market and as such, it underpins EU policy in its remit to the benefit of the Member States. Key outputs of ENISA in relation to certification are likely to enhance market conditions and help consumers and citizens alike enjoy fully the new opportunities presented by emerging technologies. The EU framework on cybersecurity certification is also an opportunity for the EU to broaden its influence far beyond its borders in a highly competitive and lucrative market where European industry can play a leading role. To this end, ENISA is able to support and enhance this European capability to the benefit of the Member States.

ABOUT ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For media enquires about this paper, please use press@enisa.europa.eu.

LEGAL NOTICE

COPYRIGHT NOTICE

Vasilissis Sofias Str 1
Maroussi 151 24
Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu