BOLSTERING ENISA IN THE EU CYBERSECURITY CERTIFICATION FRAMEWORK

EXECUTIVE SUMMARY

Against the backdrop of the Cybersecurity Act (CSA), ENISA is seeking to support the EU Member States and the European Commission in the newly defined area of European Union cybersecurity certification. The purpose of the CSA in this regard is to give a new impetus to the industry while meeting policy requirements at Member States' level. Under the CSA, the key role reserved for ENISA is to assist in the preparation of candidate cybersecurity certification schemes. In doing so, ENISA needs to interact with both EU Member States (MS) and industry stakeholders, to collect opinion and advice to feed into candidate schemes. ENISA looks forward to bolstering its role and contribute further to cybersecurity in the EU.

1. INTRODUCTION

In June 2019, the Cybersecurity Act (hereinafter CSA)[1] entered into force with a view to bring together the current cybersecurity certification activities and policies across the Member States[2]. The CSA follows an array of legal instruments that compose the legal framework of the Digital Single Market while benefiting from the framework on standardisation, laid out by means of Regulation (EU) 1025/2012[3], and provisions on conformity assessment, laid out in Regulation (EC) 765/2008[4]. This paper presents an outline of the evolving role of ENISA with regard to the emerging functions and tasks associated with the EU cybersecurity certification framework.

THE CYBER-SECURITY ACT

Under the CSA, the key role reserved for ENISA is to assist in the preparation of candidate cybersecurity certification schemes. In doing so, ENISA needs to interact with both EU Member States and industry stakeholders.

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) PE/86/2018/REV/1. Available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj

[2] European Commission, *"EU negotiators agree on strengthening Europe's cybersecurity"*, 10 December 2018. Available at: http://europa.eu/rapid/press-release_IP-18-6759_en.htm

[3] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council. Available at: http://data.europa.eu/eli/reg/2012/1025/oj

[4] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93. Available at: http://data.europa.eu/eli/reg/2008/765/oj

2. SCOPE OF CSA ON CYBERSECURITY CERTIFICATION VIS-A-VIS ENISA

The CSA is a multi-layered regulation that on the one hand addresses the updated ENISA mandate and, on the other, lays out the EU cybersecurity certification framework. ENISA is tasked with a new competence, namely to prepare candidate cybersecurity certification schemes[5]. ENISA will also assist the Commission in carrying out certain tasks (e.g. in the European Cybersecurity Certification Group (ECCG) and co-chair with the Commission the Stakeholder Cybersecurity Certification Group (SCCG)).

Thematic application areas likely to be affected by the cybersecurity certification provisions of the CSA may include specific ICT products (e.g. semiconductors), services (e.g. cloud services) and processes (e.g. information security related methods).

3. PROVISIONS IN THE REGULATION

Key limitations of the current state of affairs regarding cybersecurity certification stem from market fragmentation and uncertainty with regard to the assurance provided by existing arrangements and schemes. Concrete mitigation measures have also been deemed necessary especially in the aftermath of massive cyberattacks e.g. in the area of ransomware. With a view to pursuing the policy objective of a common cybersecurity certification framework across the EU, this new area of activity for the EU seeks to enhance the ability of consumers and EU MS governments to acquire more cybersecure ICT products, services and processes. By providing rated assurance levels, it is expected that a degree of cybersecurity commensurate with the risk profile of the application involved will be attained, thus reducing the risk footprint that would have to be mitigated by end users. It is also expected that industry operating in the EU internal market will benefit from this internal market framework and produce better outputs that stand up to global competition. With reference to ENISA, the CSA has made the following provisions in the area of certification:

It is expected that industry operating in the EU internal market will benefit from this internal market framework and produce better outputs that stand up to global competition.

- Prepare candidate schemes or review existing ones, on the basis of:
  - The Union Rolling Work Programme (URWP) for EU Cybersecurity Certification (art 47).
  - A specific request of the Commission or of the ECCG (art. 48).
- Maintain a dedicated website providing information on (art. 50):
  - EU cybersecurity certification schemes.
  - National certification schemes replaced by EU ones.
  - A store of EU cybersecurity certificates and EU statements of conformity.
- While carrying out its tasks take into account the requirements on:
  - Security objectives of EU cybersecurity certification schemes (art. 51)
  - Assurance levels (art. 52)
  - Elements of EU cybersecurity certification schemes (art. 54)
- Participate in the peer review of National Cybersecurity Certification Authorities (art. 59).
- Assist the Commission to provide secretariat to the ECCG (art. 62(5)).
- Along with the Commission, co-chair the SCCG (art. 22(4)).
- Provide secretariat to the SCCG (art.22(4)).

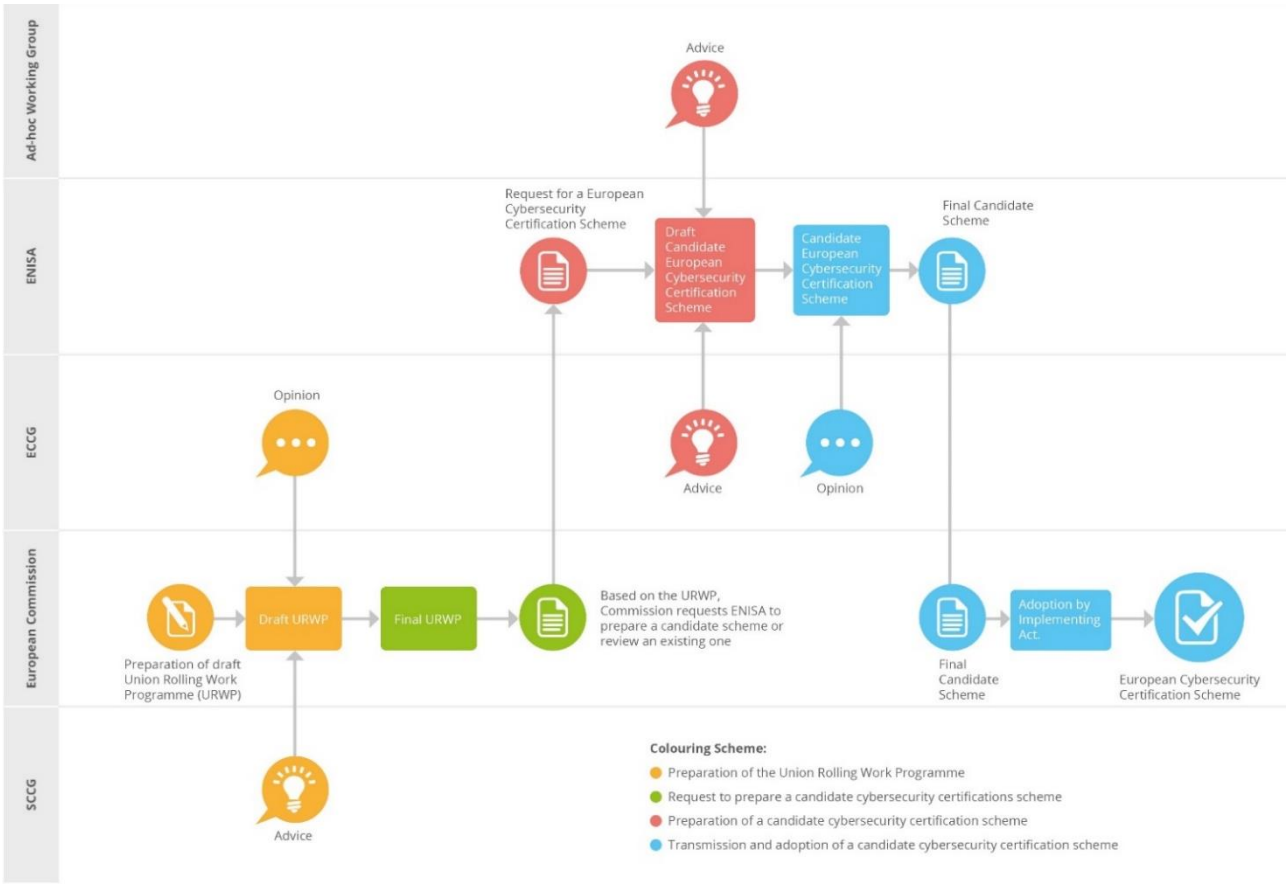
[5] CSA art. 48, 49 & 50.

- During the drafting of or each scheme, to establish an ad hoc Working Group to provide ENISA with advice (art. 49(4)).

It must be noted that the EU cybersecurity certification framework as such, does not introduce directly operational cybersecurity certification schemes.

In terms of a sequence of actions, the Commission prepares the URWP, taking into account the opinion of the ECCG and the advice of the SCCG. Thereafter, ENISA prepares schemes taking into account the advice provided by the ECCG and by an ad hoc working group per scheme. ECCG will provide an opinion at the final draft of the scheme. While such opinion is not binding upon ENISA, it is expected that it will be listened to, as a candidate certification scheme will be scrutinised by EU Member States prior to being voted as an Implementing Act. Figure 1 below illustrates this process.

Figure 1: Overview of the design of a European Cybersecurity Certification Scheme



4. STAKEHOLDERS

The role of ENISA relies on key stakeholders that include but are not limited to the following ones:

- the members of the ECCG and the SCCG,
- the European Commission and competent authorities in the Member States represented thereto,

- 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.

5. THE GOALS OF ENISA

At this stage, ENISA aligns itself with the framework and it is prepared to develop its capabilities further to respond to the new tasks in relation to cybersecurity certification. The trust that the EU Member States and the EU Institutions have vested in ENISA provides the basis to meet evolving cybersecurity challenges.

It is important to facilitate Member States, particularly those with a robust presence in information security certification, to transition to the new EU framework. The SOG-IS agreement[6] has provided the framework needed, and has proved a great success for EU industry that now needs to be taken up at the EU level. ENISA stands clear to support the transition to the new framework. Understanding the requirements of the key stakeholders in the Member States, the EU Institutions and the industry remains an important target. 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 will enable a quick response to requests to draw up candidate certification schemes.

ENISA MISSION
To pro-actively contribute to the emerging EU framework for the ICT certification of products and services and carry out the drawing up of candidate certification schemes in line with the Cybersecurity Act, and additional services and tasks.

6. MISSION

The mission of ENISA in the area of the EU cybersecurity certification framework is outlined as follows: "*To pro-actively contribute to the emerging EU framework for the ICT certification of products and services and carry out the drawing up of candidate certification schemes in line with the Cybersecurity Act, and additional services and tasks*".

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 agency that engages with public services as well as with industry and standardisation organisations, provides a sound reference point to draw up candidate cybersecurity certification schemes. The expected output of ENISA includes draft and finalised candidate schemes for the certification of ICT products, services and processes, within the meaning of the CSA.

7. CONCLUSIONS

The emerging EU cybersecurity certification framework provides ENISA with the opportunity to step up its contribution to policy on cybersecurity in the EU. Stakeholder involvement is key,

[6] The Senior Officials Group – Information Systems Security (SOG-IS) agreement has been developed pursuant to the EU Council Decision 92/242/EEC of 31 March 1992 in the area of security of information systems; it also follows on Council recommendation 1995/144/EC of 7 April 1995 on common information technology security evaluation criteria. The SOG-IS agreement was last updated in 2010.

much as guidance from the EU institutions and EU Member States are. As ENISA has been established as a support measure in the internal market,[7] it underpins EU policy within its remit to the benefit of the Member States. Key outputs of ENISA in relation to cybersecurity certification are likely to enhance market conditions and help consumers and citizens alike enjoy better opportunities presented by emerging technologies. The EU cybersecurity certification framework 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. With this bolstered role, ENISA looks forward to supporting and enhancing the capability of the EU to the benefit of the Member States.

[7] Judgment of the Court of Justice of the European Union (Grand Chamber) of 2 May 2006, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, Case C-217/04.