REPONSE ENISA SUR CERTIFICATION

I would like to thank you for questions related to the newly adopted EU cybersecurity certification framework under the Cybersecurity Act - Regulation (EU) 2019/881. As the Regulation has already entered in force, ENISA and all relevant stakeholders identified, directly and indirectly, seek to adhere to relevant provisions, processes and procedures.

The EU cybersecurity certification framework will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. Such schemes, once adopted at EU level, for specific products, services or processes, will be valid and equally recognised across all EU Member States. Currently, the landscape of cybersecurity certification of ICT products and services in the EU is quite disperse as there is a number of national initiatives and also international ones, such as the so-called Common Criteria (CC) for Information Technology Security Evaluation. The most prominent example at EU level in this regard is the Senior Officials Group – Information Systems Security (SOG-IS) Mutual Recognition Agreement (MRA). Following a direct request of the European Commission to ENISA, a successor of SOG-IS MRA will be the first scheme to be drafted within the scope of the EU cybersecurity certification framework.

European cybersecurity certification schemes could allow for both conformity self-assessments and certifications, where evaluation will be performed by third party conformity assessment bodies. In total, three assurance levels are foreseen and each one of them provides a corresponding rigour and depth of the evaluation of the ICT product, ICT service or ICT process. Through conformity self-assessment only basic assurance level can be achieved, while for certifications basic, substantial or high assurance level can be achieved. The certification process, contrary to the conformity self-assessment, adheres to the provisions on Regulation (EC) 765/2008 which sets outs requirements on for accreditation and market surveillance.

Within the scope of the aforementioned Regulation, each Member State nominates one National Accreditation Body (NAB), which grants accreditation certificates to conformity assessment bodies (CABs). The accreditation can be issued to the conformity assessment bodies for specific cybersecurity certification scheme(s), for a maximum of five years and may be renewed afterwards.

For each European cybersecurity certification scheme, the national cybersecurity certification authorities shall notify the European Commission of the conformity assessment bodies that have been accredited. Given the EU-wide validated of both the EU cybersecurity certification framework and the issued certificates, a producer or manufacturer of an ICT product, ICT service or ICT process can request an assessment process by any accredited conformity assessment body across the EU.

I hope this helps.

Best regards,