Ref. Ares(2025)5070064 - 25/06/2025

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

Ms Christiane Kirketerp de Viron
Acting Director
Digital Society, Trust and Cybersecurity
DG CNECT
European Commission

Sent via ARES in reply to Ares(2025)3345171 **Athens, 23/06/2025**

Subject: Reply of ENISA to the request for the preparation of a candidate Managed Security Services certification scheme under Article 48(1) of Regulation (EU) 2019/881 (Cybersecurity Act)

Dear Ms Kirketerp de Viron,

Let me thank you for the request of the European Commission to ENISA seeking support in the context of the certification of Managed Security Services (MSS) noting its role in the proposal for the Cyber Solidarity Act, Regulation (EU) 2025/38 (CSoA), which entered into force on 4 February 2025.

ENISA Management Board on the 17th of June 2025 acknowledged the significance of the request for the EU cybersecurity ecosystem. Thus, after receiving endorsement of the Management Board last week, ENISA can now accept the request albeit dependent on resourcing priorities as those emerge within SPD2025-2027 and observations brought out below, which in the view of ENISA Management Board will facilitate further the timely response of ENISA to the Commission request.

ENISA welcomes the request and confirms its readiness to initiate the preparation of the candidate scheme. In line with the SPD2025, ENISA has already earmarked resources for the preparation of the scheme and the feasibility study and we thank both Commission and the Member States for their support and appreciation of this preparatory work. ENISA's efforts will build on the results of the feasibility study carried out in 2024 and 2025, which was developed with the support of a thematic group composed of Member State experts.

In accordance with your request and the study, the proposal is for a **layered certification approach** for MSS, consisting of a **horizontal set of common requirements** and a **series of verticals**. These verticals define specific technical and operational requirements, some of which may be shared across multiple verticals. Given the vast scope of the first vertical as per your request, namely incident management, and in order to cater for timely delivery of the candidate scheme, we propose to follow a gradual approach of building several **Service Profiles** that will collectively constitute the incident management vertical. This approach will also ensure alignment with existing schemes such as the EUCC. In this respect, the different verticals will be composed of different **Services** that we will designate as **Service Profiles**.

As outlined in the study, the **incident management lifecycle** comprises multiple Service Profiles, including **Threat Detection**, **Incident Qualification and Escalation**, **Incident Response**, **Recovery**, and **Post-Incident Analysis**. ENISA proposes to commence and prioritize the work with the **Incident Response** Service Profile and to address the remaining profiles in a progressive manner. The

prioritisation of future Service Profiles will be done in close coordination with the European Commission and is based on the needs of the Cybersecurity Reserve as already indicated by the services offered under the ENISA Support Action.

ENISA notes that some Service Profiles—such as Detection and others relying on cloud-based infrastructure—are closely interdependent with the underlying architecture and service models addressed by the forthcoming European Cloud Services (EUCS) scheme. To ensure alignment and consistency across certification frameworks, ENISA will initiate work on these EUCS-dependent Service Profiles once the EUCS scheme has been adopted. We thus look forward to continuous collaboration with your services to finalize the adoption of the EUCS scheme.

In parallel, ENISA, under the guidance of Commission services and building on the excellent collaboration of the two teams, will conduct an analysis of relevant legislative frameworks—including the Digital Operational Resilience Act (DORA), the NIS2 Directive, among others. The aim is to promote coherence and prevent unnecessary regulatory overlap, with particular attention to ensuring that certification requirements do not create undue complexity for companies, especially small and medium-sized enterprises (SMEs).

We are looking forward to discussing the terms of reference for the respective ad hoc working group and an implementation timeline. Accordingly, ENISA will launch an Ad Hoc Working Group under the relevant provisions of the CSA to support the preparation of the scheme and will ensure close cooperation with the Commission and Member States throughout the process.

Please note that the response of ENISA to this Commission request will be carried out in the Cybersecurity Certification Unit; Apostolos Malatras, Head of Unit, remains at the disposal of your services for any further clarifications due and a follow up.

In line with the above-mentioned observations, let me confirm to you that my staff and I are prepared and available to support the Commission in its request concerning a cybersecurity certification scheme on MSS to the benefit of the EU Member States citizens and businesses, alike.

Yours Sincerely,

[electronically signed]

Juhan Lepassaar
Executive Director

C.c.: S. Schuster, R. Stefanuc, A. Wawrzyk, I. Lauringson, A. Nevado, F. Weprajetzky
A. Malatras, P. Blot

Electronically signed on 23/06/2025 12:50 (UTC+02) in accordance with Article 11 of Commission Decision (EU) 2021/2121