



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EU CERTIFICATION SCHEME ON MANAGED SECURITY SERVICES

Vicente Gonzalez Pedros
Cybersecurity Certification Unit – ENISA

EC request for an EU MSS certification scheme

NOTE FOR THE ATTENTION OF JUHAN LEPASSAAR,
EXECUTIVE DIRECTOR OF THE
EU AGENCY FOR CYBERSECURITY (ENISA)

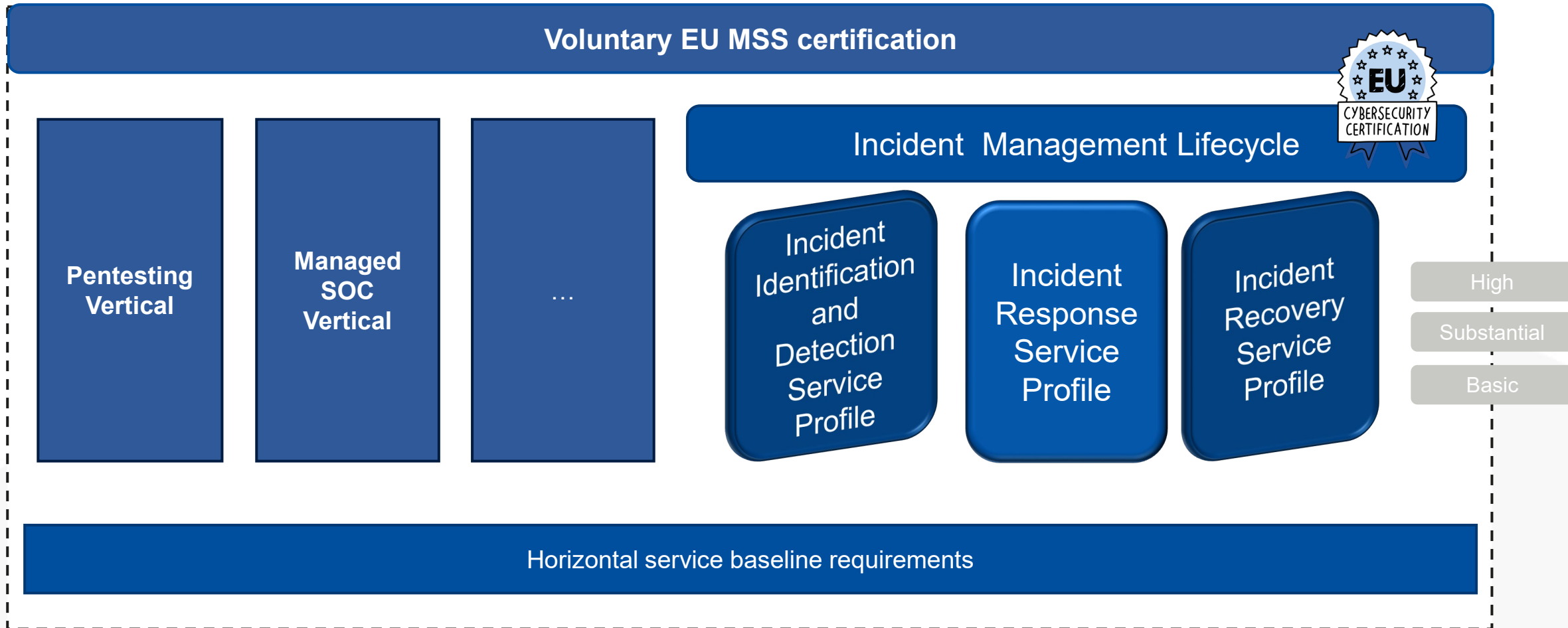
Subject: Request for the preparation of a candidate Managed Security Services certification scheme under Article 48(1) of Regulation (EU) 2019/881 (Cybersecurity Act)

Pursuant to Article 48(1) of the Cybersecurity Act (CSA), the European Commission hereby requests ENISA to prepare a candidate European cybersecurity certification scheme applicable to Managed Security Services (MSS).

Key elements

- Request focuses on **Managed Security Services (MSS)** building on amendment of **CSA Regulation (EU) 2025/37**
- Request **received on 25/04/2025**
- Request shared with ECCG on 30/04/2025
- Request **in line with URWP**
- Significant to **operationalization of CSoA** that came into force on 04/02/2025
 - Trusted **MSSPs have to be certified in accordance with EUMSS**, 2 years after scheme is in place
- National schemes already in place; risk of fragmentation

SCOPE AND STRUCTURE OF EUMSS CERTIFICATION



Commission Request to ENISA for a cybersecurity certification scheme on EU MSS

Horizontal Layer

Common baseline requirements; not a stand-alone certification but a prerequisite for every vertical pillar.

Objectives = ensure secure-by-design delivery, seamless client integration, resilience to disruption, and robust lifecycle management.

Vertical Layer

Annexes to the horizontal layer that add MSS-specific technical requirements per service domain.

- **Scope** = Incident Management - full lifecycle (identification/detection, response, recovery, post-incident review), with requirements for reporting, escalation, stakeholder coordination, and continuous improvement
- **Objectives** = Provide precise criteria tailored to each MSS characteristics and risk profile; certification labels are MSS-specific.

Status update of EUMSS

ENISA ANSWER TO EC REQUEST

Follow a gradual approach of building several Service Profiles that will collectively constitute the incident management vertical

Commence and prioritise the work with the Incident Response Service Profile

EUMSS AHWG

The AHWG drew on a pool of 200+ applicants to appoint outstanding, senior-level MSS professionals – in total 60 members including representatives of MS

Meets regularly physical but also online

CURRENT STATUS

Development of the scheme in progress

- Collaboration with appointed industry (AHWG) experts and Members States
- Horizontal Layer and Vertical pillar requirements as well as audit guidance on the basis of ISO TS18072 standard

TIMEPLAN

20/03/2026

09/4/2026

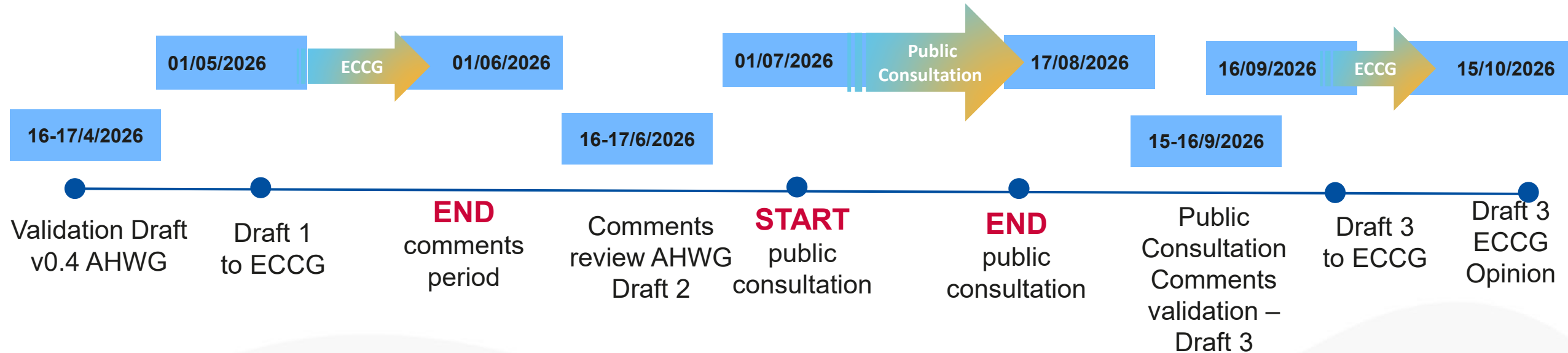
Main Scheme Draft v.03
sent to AHWG

250 Comments Received

- Relationship with NIS2.
- Assurance Levels for Multiple Profiles.
- Evaluation Standards and Methodologies.
- Cross-Border Oversight.
- Terminology Alignment.
- Certification Scope (Client-Specific vs. General).
- Evaluation Repetition Costs.
- NCCA and CAB Dialogues.
- Confidentiality in Certification Reports.

Main Scheme Draft v.04
Sent to AHWG

TIMEPLAN



Stay tuned and have your say –
Public Consultation beg. July-
end Aug

**Follow the updates on
Certification website**

[Homepage - European Union Cybersecurity
Certification - European Union](#)

[2026 European Cybersecurity Certification Conference - European Union
Cybersecurity Certification](#)



Thank you for your attention



certification.enisa.europa.eu

ENISA

European Union Agency
for Cybersecurity

Athens Office

Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office

Rue de la Loi 107
1049 Brussels, Belgium