REQUEST FOR COMMENT RESPONSE

Proposal for a Regulation on the EU Cybersecurity Act

12 May 2026

CrowdStrike EU Transparency Register Nr. 659664851434-16

I. INTRODUCTION

In response to the European Commission's (EC) request for feedback on proposed Regulation on the EU Cybersecurity Act 2 ("CSA2), CrowdStrike offers the following views.

We approach these comments as a leading international, U.S.-headquartered, cybersecurity provider that defends enterprises from globally distributed threats. Our AI-powered, cloud-native platform delivers state-of-the-art, real-time detection, automated protection, and threat intelligence across endpoints, cloud, identity, data, and AI workloads. Our insights are informed by applied, real-world experience across global industries through our software-as-a-service cybersecurity platform, incident response, managed threat hunting, and managed security services. CrowdStrike's recommendations are grounded in this operational experience.

II. COMMENTS

CrowdStrike supports the Commission's objective to clarify and adapt the mandate of ENISA, improve the European Cybersecurity Certification Framework (ECCF), and reduce fragmentation in the EU cybersecurity rulebook. For modern cybersecurity, however, the Regulation should preserve outcome-based rules that can keep pace with AI-enabled attacks, cloud-native architectures, managed security services, and rapidly evolving adversary tradecraft. The most effective framework will deepen structured public-private cooperation, align with international standards, and allow entities in the Union to use the best available cybersecurity services without unnecessary duplication or delay.

As drafted, several provisions may risk undermining those goals. The proposal would benefit from clearer stakeholder governance, firmer limits on ENISA's role in standard-setting, more workable certification development timelines, stronger

interoperability with adjacent EU cyber laws, and tighter safeguards around the ICT supply chain framework so that non-technical risk measures remain evidence-based, proportionate, and predictable. Simplification should mean that defenders spend less time repeating audits, reporting, and certification steps, and more time preventing, detecting, and responding to threats.

While we do not have feedback on every aspect of the proposed act, we do want to offer several points that may be of value to the EC as it considers the proposal.

III. RECOMMENDATIONS

1. Strengthen structured stakeholder participation in ENISA and ECCF governance (Articles 35, 72 and 74).

Under Title III (European cybersecurity certification framework) and the related governance provisions in Title II, CSA2 should revise Article 72 (European Cybersecurity Certification Assembly), Article 74 (Preparation, development and maintenance of European cybersecurity certification schemes), and Article 35 (ENISA Advisory Group) to strengthen structured stakeholder participation. This is necessary to ensure that ENISA and the ECCF remain effective, technically credible, and responsive to a fast-evolving threat landscape in which cybersecurity capabilities, services, and attack techniques develop far more quickly than static governance cycles.

- Article 72 should therefore require balanced and expressly identified stakeholder representation in the Assembly, including ICT providers, cloud and digital service providers, and managed security service providers. Article 72 should also require the Assembly to maintain structured contact with stakeholders more frequently than through a single annual meeting.
- Article 74 should be amended to establish a standing stakeholder mechanism that enables continuous expert input during the development and maintenance of schemes, rather than relying only on ad hoc consultations.
- Article 35 should be revised so that ENISA's Advisory Group may advise on Title III and Title IV (Security of ICT supply chains).

Regular and representative engagement of this kind would improve the quality, feasibility, and relevance of EU cybersecurity policy by ensuring that certification and guidance are informed by practical expertise on emerging threats, operational realities, and unintended implementation burdens.

2. Keep ENISA in a technical support role in standardisation and make ENISA-drafted technical specifications exceptional and temporary.

Under Title II and the certification-related provisions of Title III (European cybersecurity certification framework), CSA2 should clarify through Article 18 (ENISA's role in standardisation) and Article 77 (technical specifications) that ENISA's role is to contribute technical expertise, legal-technical guidance, and support for the assessment of standards, but not to operate as a parallel European standards body or to assume a lead role in standardisation processes that should remain open, consensus-based, and industry-led.

Article 77 should therefore be revised so that ENISA-drafted technical specifications are created when no relevant European or international standard exists, or where a documented and urgent security need makes timely reliance on standards impossible. . This process would preserve the integrity of the international and European standardisation system while still allowing urgent technical gaps to be addressed in a targeted and proportionate manner. It would also reduce the risk of conflicting technical rulebooks, support interoperability across borders, and ensure that certification remains anchored in recognised European and international standards that can evolve with modern security technologies and services.

3. Make certification schemes agile, risk-based, and fit for modern cybersecurity services, especially managed security services.

Where certification schemes under Title III (European cybersecurity certification framework) are used to demonstrate compliance with Article 21 NIS2 cybersecurity risk-management measures, any 'cyber posture' certification should remain outcome-based, risk-driven, and operationally feasible, so that it reflects real security outcomes rather than static checklists. Effective certification schemes accommodate different operating models, threat exposures, and continuously updated cloud-native environments.

Under Title III (European cybersecurity certification framework), CSA2 should ensure that Article 74 (preparation, development and maintenance of European cybersecurity certification schemes), Article 81(3) (national extension profiles), Article 82(7) (high-assurance assessments), Article 86(3) (transition or grandfathering of existing

certificates), and Article 87 (international recognition) support certification schemes that are agile, transparent, and responsive to real-world risk:

-
- The proposal should require at least one formal stakeholder consultation opportunity after a candidate scheme has been developed and before adoption, together with greater transparency on draft texts, milestones, and expected timelines. For managed security services, certification pathways should be risk-based, and certification should become mandatory only where a service-specific and sector-specific risk assessment demonstrates a clear need after stakeholder consultation.
- Where schemes address cyber posture or managed security services, they should reflect contemporary defensive capabilities including cloud security, Endpoint Detection and Response (EDR), AI Detection and Response (AIDR), Identity Threat Detection and Response (ITDR), and where appropriate, next-generation SIEM. Contemporary practices should include the use of Zero Trust architectures, extensive logging, threat hunting, and where appropriate, 24/7 managed services.
- Article 81(3) should clarify that any Member State extension profile must remain strictly technical and may not recreate divergent legal effects around the same EU certificate; and
- Article 86(3) should preserve grandfathering for existing certificates.
- Article 87 should support international recognition and reduced assessment scope where equivalent international certifications already exist; and
- Article 82(7) should be reconsidered, or at minimum conditioned on a formal capacity assessment, so that high-assurance assessments are not bottlenecked by an insufficient pool of EEA-based conformity assessment bodies.

These changes would make certification more credible and usable by aligning it with the operational realities of cloud-native, modular, and AI-assisted cybersecurity services, rather than forcing dynamic security capabilities into static or outdated models.

4. Use CSA2 as a simplification tool across the EU cyber acquis, not as a new layer of duplicative compliance.

Under Title III (European cybersecurity certification framework) and the related recitals, implementing provisions, and ENISA guidance mechanisms, CSA2 should expressly support simplification across overlapping EU cybersecurity laws rather than adding a further compliance layer:

- The regulation should include operative language clarifying that EU cybersecurity certificates and cyber posture assessments may, where underlying controls are equivalent, serve as evidence of compliance across overlapping frameworks including NIS2, DORA, and the Cyber Resilience Act .
- Implementing acts and ENISA technical guidance should also support the mutual recognition of overlapping audits, testing, and documentation, so that entities are not required to demonstrate the same controls multiple times under different Union instruments.
- Where ENISA develops digital interfaces, templates, or supporting technical arrangements, these should be built around a "report once, comply many" principle and should not create parallel reporting or evidence channels for substantially similar obligations.
- Where the Commission adopts implementing acts on cybersecurity risk-management measures, CSA2 and the related NIS2 simplification provisions should preserve maximum harmonisation so that Member States do not impose additional technical, methodological, or sector-specific requirements on entities already covered by those acts. Those implementing acts should be developed through an open, transparent, and inclusive consultation process and should remain updateable so that harmonised requirements can keep pace with adversary innovation, technological change, and operational practice.

This approach would direct cybersecurity expertise toward threat detection, resilience, and incident response rather than repetitive administrative exercises, which is particularly important for SMEs, for entities operating across several regulated sectors, and for providers supporting customers under multiple legal regimes. CSA2 should therefore reinforce the simplification direction identified in the broader EU digital simplification agenda and reduce friction at the point of implementation.

5. Tighten the ICT supply chain framework so it remains evidence-based, proportionate, and technically anchored.

Under Title IV (Security of ICT supply chains), CSA2 should refine Article 99 (security risk assessments), Article 100 (designation of third countries posing cybersecurity concerns), Article 103 (mitigation measures), Article 104 (identification of high-risk suppliers), and Annex II (key ICT assets for mobile and fixed electronic communications networks) so that supply-chain interventions are predictable, evidence-based, and proportionate to actual cybersecurity risk:

- Article 99(3) should define more clearly the threshold for Commission-led security risk assessments, including what constitutes a "significant cyber threat" and "sufficient reason to believe," and should include a clear timeline comparable to the process in Article 99(2).
- Article 100 should be revised so that any third-country designation is based on objective and cumulative criteria.
- Article 103 should require a documented technical and economic impact assessment, consideration of available alternatives, and workable transition periods before any restriction or replacement obligation takes effect, and restrictions should not automatically apply to technical certification or managed security services without a specific risk finding.
- Article 104 should define "establishment" and "control" narrowly and should not use the nationality of individual employees or directors as a proxy for cybersecurity risk; equally, non-cooperation should not create an automatic presumption of high-risk status without due process and an opportunity to respond.
- In implementing Title IV (Security of ICT supply chains), the Commission should use the ICT Supply Chain Security Toolbox to operationalise simplification and avoid repetitive supplier assurance exercises. Commission guidelines should standardise the structure and level of detail of supplier assurance requests, encourage re-use of common inputs across customers, and align assessments with scenario-based and lifecycle-oriented risk management.
- Annex II should also be revisited so that key ICT assets are identified only following asset-specific risk assessment and proportionate mitigation analysis, rather than through broad ex ante inclusion of fixed and related categories without the necessary sectoral evidence.
- CSA2 should also promote diversification and interoperability as core resilience outcomes by encouraging proportionate multi-vendor strategies, open standards, and secure-by-design approaches that reduce lock-in, enable entities to maintain resilient multi-supplier environments and reduce risks without

compromising security. CSA2 should also recognise procurement as a practical resilience lever by encouraging cybersecurity-related requirements and award criteria that support secure, interoperable, and resilient supply chains.

A more targeted framework of this kind would better protect the Union by focusing intervention where real risk is demonstrated, while avoiding unnecessary disruption, preserving access to trusted cybersecurity services and technologies, containing compliance costs, and supporting innovation and operational resilience across the Single Market.

IV. CONCLUSION

The EC's proposed regulation provides a thoughtful analysis of a complex legal and policy area. As updates to the law and administrative rulemaking moves forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any legislative updates and proposed rulemaking focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

V. ABOUT CROWDSTRIKE

CrowdStrike (NASDAQ: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft, and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting, and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity, and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/.

CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley
Chief Privacy and Policy Officer

Līga Rozentāle
Director, Head of Public Policy, EMEA

Email: policy@crowdstrike.com