Council of the European Union
General Secretariat

Brussels, 10 December 2025

WK 17169/2025 INIT

LIMITE

CYBER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Horizontal Working Party on Cyber Issues
Subject:	Non-Paper on the Revision of the Cybersecurity Act - Spain's position

Delegations will find in the annex a non-paper by Spain on the revision of the Cybersecurity Act.

Non-Paper on the Revision of the Cybersecurity Act

SPAIN'S POSITION

In anticipation of the upcoming revision of the Cybersecurity Act (CSA), the Spanish authorities have coordinated to define a common position to be conveyed to the European community.

Spain has conducted an in-depth analysis of the various non-papers submitted by several Member States in the context of that revision and, in broad terms, aligns with many of the points included in the "Joint Non-Paper on the ENISA Mandate" endorsed by twenty Member States. Building on that document, Spain wishes to reiterate its support while adding two additional recommendations.

The recommendations of this non-paper therefore focus on the following areas:

I. ENISA's mandate

II. Improving the governance of the European Cybersecurity Certification Framework

Spain considers that strengthening Europe's digital resilience requires a clear, stable and forward-looking cybersecurity framework. In an increasingly complex threat landscape, the European Union must remain committed to promoting trust, safeguarding innovation and ensuring that citizens and companies can rely on secure digital technologies. Spain supports the shared objective of consolidating the European Union as a sovereign, leading global actor in this domain, based on a strong protection and resilience against cyber risks and on an ambitious regulatory framework coherent and proportionate to varying risk levels. The NIS 2 and CRA Directive are milestones in this effort.

I. ENISA'S MANDATE

1. **Joint Non-Paper on the ENISA Mandate in the revised Cybersecurity Act signed by Austria, Belgium, Bulgaria, Croatia, Czech Republic, Estonia, Finland, France, Germany, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Slovakia and Slovenia.**

Spain supports the references concerning the centre of expertise, EU common situational awareness and operational cooperation, strategy and governance. Spain highlights the following elements:

- *ENISA should strengthen its role as a centre of expertise on cybersecurity supporting the Member States, serving as a hub for knowledge, information aggregation and diffusion at the EU level. ENISA should also continue to enable and promote the effective implementation of EU cybersecurity legislation with the highest priority.*

- *ENISA should remain the enabler of EU cooperation. We do not consider, however, that it should aspire to become a Union level CSIRT. ENISA should rather focus on strengthening its tactical role in operational cooperation through support for the CSIRT Network and the EU-CyCLONe, as well as being part of the EUIBAs framework as well as on supporting national CSIRTs and cybersecurity authorities. Finally, it should facilitate further cooperation within the networks, in particular taking into account the EU Cyber Blueprint.*

- *ENISA is best positioned to support the development and coordinate EU common situational awareness capabilities and actively facilitate structured information exchange within the CSIRTs Network and EU-CyCLONe. ENISA is best positioned to consolidate and complement, on the basis of information gathered from various sources, the analyses produced at national level. This requires a clear and transparent information management strategy, to be endorsed by the Management Board, guiding how ENISA organizes, processes and disseminates information received from Member States and other trusted partners.*

- *The mandate of the ENISA Management Board should be strengthened to reflect its role as the body establishing Agency's priorities and providing guidelines for its everyday work. ENISA should not be given additional tasks without prior consultation and agreement of the Management Board, as this undermines the Management Board's central role.*

- *To this end, the Management Board should convene at least once or twice a year for a strategic discussion on the Agency's priorities and developments. Given its limited resources, careful periodical prioritization and de-prioritization by the Management Board is necessary. Findings from that discussion should be integrated into the Single Programming Document.*

- *To ensure that ENISA can effectively deliver on its mandate, it is essential that the Agency is provided with stable, adequate, and long-term resources and funding. The framework needs to guarantee the Agency's ability to retain institutional knowledge, develop long-term expertise, attract the required talent and invest in strategic priorities. ENISA should maintain infrastructure and critical information systems through in-house resources, having a high security in accordance with the EUIBAs Cybersecurity Regulation. Permanent funding that reflects ENISA's role in the EU's cybersecurity architecture is crucial.*

2. ENISA's collaboration with the Military CERT Network (MICNET)

Spain proposes introducing an explicit reference to the EU Military CERT Network (MICNET) in the revised CSA and reflecting it appropriately in ENISA's mandate and / or objectives.

This update is necessary to reflect the current cyber-defense architecture of the Union and to ensure coherence between the different regulatory instruments and operational structures that have developed since 2019. This proposal is anchored in the strategic context of the 2020 EU Cybersecurity Strategy, the 2022 EU Cyber Defense Policy, and the EU Cyber Blueprint, all of which emphasize the need to reinforce cooperation between the civilian and military cybersecurity and cyber-defence communities.

At the time of adoption the CSA, MICNET had not yet been implemented. Today it constitutes an essential component of the Union's cyber-defense ecosystem. Recital 43 of the CSA already recognizes cooperation with international partners, including NATO. Extending this logic to explicitly reference MICNET would be a natural evolution.

Incorporating MICNET in the CSA would:

- strengthen structured civil–military cooperation mechanisms.

- enhance situational awareness and operational coherence across cybersecurity and cyber-defense actors.

- support a more integrated Union response in the event of large-scale incidents affecting defense systems.

- ensure that ENISA informs MICNET military CERTs, where necessary and on a case-by-case basis, of matters that may affect national defence.

3. ENISA's collaboration with European Cybercrime Centre (EC3)

ENISA shall cooperate, where appropriate, with Europol, particularly through the European Cybercrime Centre (EC3), to enhance situational awareness, the exchange of threat information, and the coordinated response to cross-border incidents with a criminal dimension.

4. Capacity building and cybersecurity maturity

Spain considers essential to strengthen Europe's overall maturity through capacity-building programs focused on training, awareness and tooling. These programs are fundamental to consolidating a cohesive and resilient European cybersecurity community.

II. IMPROVING THE GOVERNANCE OF THE EUROPEAN CYBERSECURITY CERTIFICATION FRAMEWORK

To optimize the European Cybersecurity Certification Framework, Spain has analysed various governance models across the EU acquis (NIS Cooperation Group, CyCLONe, European AI Board, EDPB). Spain proposes a model based on three pillars:

- Permanent presidency by the European Commission.
- Technical authority in the hands of Member States.
- Voting mechanisms with defined deadlines.

This structure would enhance ECCG's effectiveness, ensure consistency and avoid regulatory fragmentation.

Spain acknowledges the efforts of the European Commission and the key role played by ENISA in preparing technical work and drafting schemes. However, the current functioning of the ECCG (based on non-binding views and lengthy deliberative processes) has proven insufficiently agile. In a rapidly evolving technological environment, this lack of speed risks undermining the timely development of certification schemes and their effective implementation.

Spain considers that the new, reformed model should be characterized by:

- Effective integration of national expertise, going beyond the current advisory role.
- Stronger decision-making power for the ECCG, reflecting Member States' competences and responsibilities.
- Agility, enabling the framework to address urgent regulatory and market needs.
- The imminent applicability of the CRA and the CSA reinforces the need for a robust, stable and agile framework, given the compressed timelines, growing threat landscape and expanded compliance obligations.

A renewed governance model is essential to make full use of national authorities' experience and to ensure the operability of the ECCG. It would also facilitate transitional mutual recognition arrangements to mitigate regulatory gaps until the European framework is fully implemented.

Description of the Proposed ECCG Model

It is advisable that the ECCG presidency remains in the hands of the European Commission, which would assume the role of secretariat and permanent coordinator. This continuity will enable the maintenance of a coherent strategic agenda. However, the agenda should not be rigid: Member States would retain the ability to request the inclusion of new items through a formal procedure, ensuring that national priorities are duly reflected in the group's work.

Technical leadership would lie with the competent authorities of the Member States, organized in permanent thematic sub-groups created, or to be created, in connection with European cybersecurity schemes. These sub-groups would address critical areas such as software, hardware, cloud services, AI, and alignment with other European regulations such as the Cyber Resilience Act. They would form the core of the technical development process, generating proposals for discussion and voting within the ECCG.

Their work may draw on information and analysis provided by the Information Sharing and Analysis Centres (ISACs), leveraging their experience in identifying emerging risks and sectoral trends. For example, the work of the ISAC linked to the EUCC scheme—already established—provides technical intelligence relevant to ICT product certification and should be considered. This collaboration would allow sub-group proposals to reflect real market needs and current threats, without compromising the decision-making authority of the Member States within the ECCG.

To strengthen the effectiveness of the process, a simple majority voting should be the general rule for procedural and operational matters, as well as for proposals for new schemes. All major decisions taken within the group should in any case be subject to a vote, requiring a simple majority of votes cast, except for the technical approval of an already developed scheme, which should be adopted by consensus. A vote should also be held whenever a Member State formally requests it in relation to any decision within the ECCG.

Technical proposals should be put to a vote, with a maximum period of thirty days for their adoption. Decisions adopted by formal vote within the ECCG should be respected by the Commission, which should incorporate them into certification schemes and operational decisions.

To ensure agility and transparency, proposals subject to voting should be submitted through the group's digital platform, using a standardized format including: a clear title, technical justification, expected impact on the harmonization of schemes, and, where appropriate, regulatory references. Once submitted, the proposal would be published for consultation and discussion for a maximum period of fifteen days, after which electronic voting will open for a defined period (e.g. thirty days). Proposals reaching the required majority should be respected by the Commission and integrated into the ECCG's work. This procedure aims to strike a balance between open participation and the need for swift and operational decision-making.

Where approval of a certification scheme for ICT products, services or processes or regulatory changes could result in the loss of validity of a national certification scheme, Member States may request that the ECCG carry out an assessment, and subsequently, where appropriate, request a vote to determine whether the conditions set out in Article 57 of the CSA are met.

In the event of a discrepancy between the majority view of the ECCG and the position of the Commission, a formal conciliation procedure should be established. A final decision should not be taken without an explicit agreement reached through this process. Such an arrangement would ensure that the ECCG—and thus the collective position of the Member States—cannot simply be disregarded, and that the Commission is encouraged to explain and substantiate its position in writing. This mechanism would also ensure that disagreements are clearly identified and reasoned, enabling Member States to participate actively and effectively in decision-making.

Spain therefore proposes that the mechanism to resolve discrepancies be explicitly defined to facilitate support from both Member States and the Commission, by:

- Setting out that ENISA may reject ECCG requests only on limited and well-justified grounds, such as:
    - Insufficient technical resources.
    - Overlap with a scheme already under development.
    - Incompatibility with existing EU legislation.
- Requiring that any rejection be reviewed by the Commission within a defined deadline, following formal consultation of the ECCG.
- Requiring that, if the Commission confirms the rejection, it provides a public and reasonable explanation in writing.
- Allowing the ECCG, as a last resort, to refer the matter to ENISA's Management Board (where Member States are represented) with a view to overturn the Executive Director's decision.

Moreover, it is essential to limit ENISA's current capacity to reject ECCG requests to prepare new certification schemes. This provision makes it explicit that the ECCG's position is not binding on ENISA. Therefore, the rule should be revised to introduce a dispute-resolution mechanism in which the European Commission plays a central role, thereby improving and streamlining the decision-making process.

1. Additional Proposals Concerning the ECCF

Spain advocates for the inclusion of three additional proposals:

- Participation of Member States in the Union Rolling Work Program (UWRP)

The Union Rolling Work Program should be examined within the ECCG before Commission approval, with the possibility for Member States to request a vote.

- Compatibility of NCCA and CAB functions

Spain proposes adding a clarification to Article 58(4) confirming that the same NCCA may perform certification and supervisory functions, provided that its independence is ensured through appropriate organizational and procedural safeguards.

- Transitional recognition of national schemes

A mechanism is required to ensure temporary EU-level recognition of national certification schemes until the European framework is fully operational.

Spain strongly supports the following improvements as well stated in the non-paper by Belgium, Croatia, Lithuania, Poland, Portugal, Slovakia and Slovenia on the European cybersecurity certification framework:

- Clarification of responsibility for maintaining schemes

The revised CSA should explicitly define whether ENISA, the Commission or the ECCG holds final responsibility for maintaining schemes and addressing insufficient maintenance or lack of budget.

- Need for a standard template for implementation acts

To improve agility and reduce duplication, the CSA should introduce a standardized template for integrating schemes into implementing acts.

- Strengthening national capabilities

The success of the ECCF depends on robust national ecosystems. Adequate EU funding should support NCCAs and CABs.

ENISA should provide tailored training, workshops and awareness-raising activities to support national authorities and industry.