# Non paper on the Review of the Cyber Security Act

## The Netherlands

## Part 1. A futureproof ENISA

Over the last decades, ENISA has proven to be an indispensable organisation within the EU cyber landscape. The expertise and decisiveness of the agency has enabled the Member States to jointly strengthen the cybersecurity level across Europe. Because of its excellent expertise and reputation in the cyber ecosystem, ENISA has been entrusted with many additional tasks over the years. Increasing demand did put an intense pressure on ENISA's involvement and resources. ENISA should remain a central player outfitted with a **futureproof**, **focused** and **clear mandate** underpinned by **sustainable funding** in the years to come. The solution should not be found in a continuous expansion of tasks, but it should focus on the areas that matter the most and where ENISA is **best equipped** to effectuate **real change** and **impact.**

### A. Most impactful priorities for ENISA

**1.ENISA as the EU centre of expertise on cybersecurity.** ENISA has provided a scala of best practices and guidelines over the last decades, which effectively boosted the cyber resilience of Member States. We strongly believe that building, connecting and sharing expertise on current cybersecurity challenges should remain a key role in its mandate, especially given the fast development of the cyber domain and the current geopolitical context. ENISA should look forward, build foresight capabilities and anticipate on the risks, threats and opportunities for cybersecurity of key emerging technologies. ENISA could also identify cybersecurity services that have a strategic impact on the mitigation of cyber threats within the Union. Non-profit organisations such as Shadowserver and Mitre are concrete examples of such services. This in order to find key insights to encourage and facilitate the Member States to build the knowledge to tackle these challenges within the Union.

**2.ENISA as enabler and promotor of effective EU cybersecurity implementation of legislation**. The primary goal of EU policy making in the upcoming years should be to fully consolidate ongoing efforts, create necessary preconditions and incentives for Member States to effectively implement cyber legislation, and reduce complexity and overlap of tasks within the EU cyber landscape. Focus on implementation, harmonization and innovation[1] are key elements and ENISA plays a crucial role in all these areas. The implementation of the CRA and the NIS2 provides significant challenges for many Member States and other organisations involved. ENISA should use the expertise and lessons learned of Member States to support voluntary harmonization in order to enable a uniform, effective and business friendly framework for cybersecurity standards across Member States. Particularly in the areas of vulnerability reporting, risk management and security requirements. ENISA should (continue) to focus on supporting the development, introduction, and promotion of standards, in collaboration with CEN, CENELEC and ETSI or other relevant international standardisation organisations, making sure that existing and emerging standards align with and support European policy, rules, and

[1] https:// eerstekamer.nl/9370000/1/j4nvgs5kjg27kof_j9vvksvji1pf4wd/vmd1h4szhtzz

regulations. Additionally, efforts of ENISA focusing on the harmonisation of data collection for CIRAS, the Common Security Advisory Framework, and the alignment of taxonomies among Member States remains important.[2]

**3.ENISA as enabler of operational cooperation between Member States.**

a. ENISA as central player within the CSIRT network and EU-CYCLONe: ENISA should reinforce the CSIRT-network and EU-CyCLONe by facilitating and fostering information-sharing between the CSIRTs and crisis management authorities. It should focus on supporting CSIRTs and crisis authorities to attain a higher level of maturity and look at ways to accelerate the cooperation within the networks. The possibility of creating a well-equipped office for the CSIRT network and EU-CyCLONe, could be explored in order to help strengthening the cooperation and information sharing between the Member States. This could on the long-term help building the capacity to quickly respond to new needs and requests within the Union.
b. ENISA as enabler of EU cooperation, not a CSIRT: ENISA is the driver of various mechanisms, such as secretary of various partnerships, and it fulfils an important role in the operation by receiving vulnerability reports and administering the EU Vulnerability Database. The reports drafted by ENISA provide valuable insights for Member States and their own operation. ENISA is however not a CSIRT and should not be tempted to take over activities of national CSIRTs that are best equipped, placed and mandated to perform these tasks. This would especially be the case with regards to operational tasks of CSIRTs such as, but not limited to, the execution of pentests, the handling of incidents, or (when asked) helping organisations recover when a major incident occurs.

**4.ENISA as information hub for a shared EU situational awareness.** ENISA has been entrusted over the years with different tasks with respect to information sharing and analysis, in close cooperation with the Member States and EU Institutions, Bodies and Agencies. Due to the complex EU cyber landscape, creating shared situational awareness remains challenging. Therefore, ENISA should be tasked to develop this common understanding and perception of risks and threats across the entire Union to support Member States and organisations to align their readiness and response. The cornerstone of this function should remain the assessments of Member States via the CSIRTs Network and EU-CyCLONe. This development should go hand in hand with the development of a comprehensive and transparent information management approach and strategy to guide how ENISA effectively collects, processes and analyses information from various sources.

**5.ENISA as support lab for cybersecurity tooling, techniques and infrastructures to support National CSIRTs**. This should aim to bring together national experts to support the joint development and harmonization of tooling and infrastructure and enhance interoperability to support the data-driven work of CSIRTs in the future.

There is a sixth activity where ENISA's efforts are crucial, ensuring the smooth function of the European Cybersecurity Certification Framework. This will be elaborated in part 2 of this non-paper.

[2] Incident reporting — CIRAS

## B. Preconditions to equip ENISA to be impactful

**6.Fully maximize the capacities of the Union by looking at ways to find synergies.** Cybersecurity expertise is very scarce within the EU. It is therefore important to look at possibilities to better streamline the roles and responsibilities of the EU agencies, in order to avoid duplication. This could for example be done by:

a. Investigating if some tasks potentially make more sense to be executed by the European Cyber Competence Center (ECCC). It could be fruitful to investigate if the ECCC could, when given sufficient capacities and resources, play a bigger role with regards to cybersecurity awareness, skills and innovation. This could be done clarifying the term 'awareness' in the CSA, which would consequently lead to better defined roles and responsibilities. Additionally, a closer cooperation between ENISA and ECCC with regards to research and innovation and market development could be considered. This can support the impact of strategic efforts, for example through improved work programs for European funding.
b. Reshaping the structured cooperation between EU agencies active in the cybersecurity domain, notably between ENISA, CERT-EU, Europol, European Defence Agency, and the ECCC.
c. Adjusting the Programme Committees for several European funding programmes targeting the cybersecurity sector (such as Digital Europe, Horizon Europe and the European Defense Fund) in order to reduce complexity, increase efficiency, support the research-innovation-maturation-deployment spectrum and create the necessary conditions for closer collaboration.

**7.Reinforce the involvement of the Member States in the preparation of the Single Programming Document.** The responsibility of preparing the draft of the Single Programming Document is now solely placed as a responsibility of the Executive Director. This program is of crucial importance because it outlines ENISA's tasks. The Management Board should play a bigger role in the drafting process, instead of only approving it. That will raise the involvement of the Member States, resulting in a closer cooperation between the Member States, ENISA and the European Commission. This could be achieved by organizing an additional session once a year, wherein this document is thoroughly reviewed with the participants. Moreover, ENISA should strengthen its role as secretary, and make sure Member States do get timely the needed documentation (agenda's, reports, summaries of the meetings) in order to fulfil their role in the decision-making process.

## Part 2. Setting the standard for European Cyber certification

The CSA introduced a harmonized European system for the cybersecurity certification of ICT products, services and processes. It ensures that manufacturers and service providers do not have to obtain a certificate in each Member State separately enhances the level of cybersecurity in the EU, supports European standardization efforts and creates a level playing field in the European internal market. This enhances the competitiveness of European businesses. The importance of cybersecurity certification and standardization will only grow in the coming years since the success of the implementation of EU legislation such as NIS2, Cyber Resilience Act (CRA), e-IDAS2 and DORA will heavily rely on effectively utilizing harmonized European cybersecurity schemes.

The European Commission's coordinating role is pivotal for ensuring consistency between legal acts that necessitate certification schemes. It has become evident that drafting and publishing schemes are challenging tasks. To ensure the effective functioning of the European Cybersecurity Certification Framework (ECCF), the Netherlands puts forward the following comprehensive and experience-based proposals and considerations to ensure a quicker and broader market uptake of the schemes and to increase the efficiency of the certification development process.

### A. Improve governance and clarity of roles and responsibilities

**8.Enable, entrust and equip ENISA** to ensure the smooth function of the ECCF. To achieve this it is important to clearly separate the roles and responsibilities between the Commission and ENISA, particularly when it comes to requesting ENISA to draft a scheme and chairing the European Cybersecurity Certification Group (ECCG).

> In addition to the drafting phase, ENISA should also be formally mandated and adequately resourced to take responsibility for the ongoing management, review and maintenance of existing certification schemes. Furthermore, ENISA should play a proactive role in promoting the uptake of these schemes across Member States and relevant market actors, including through awareness-raising, technical guidance, and stakeholder engagement. This would help to ensure that certification delivers real added value in practice and does not remain underutilized.

**9.Strengthen the decision-making of the ECCG**. The ECCG should assume a leading role in the initial evaluation of proposals concerning existing schemes. The ECCG should be able to approve or declare the proposal as controversial on the basis of majority voting. Proposals within the CSA scope must be presented to the ECCG for consideration and formally endorsed by 'voting' or 'agreement'. The European Commission constructively fulfils its role as the formal mandating authority and chair of the ECCG. A clear separation of these functions is essential to enable ENISA to effectively carry out its professional responsibilities.

**10.Fully utilize a well-defined Union Rolling Work Program (UWRP).** A joint, forward looking prioritization of schemes to be developed on the basis of Member States interest, industry needs and technological developments has not fully taken off yet. The EU, specifically the European Commission in close cooperation with ENISA and the ECCG, must possess a thorough comprehension of the schemes requiring prioritization for EU cybersecurity certification, including a strategic roadmap. In pursuit of this, due consideration should be accorded to national initiatives and market demand. Such considerations are pivotal for the purposes of harmonization.

## B. Characteristics of the ECCF: voluntary and based on technical risks

**11. Certification under the CSA should remain voluntary.** The NIS2 Directive and the CRA already impose substantial compliance obligations. Therefore it is important that certification schemes under the CSA) remain voluntary. Making CSA certification mandatory would primarily lead to increased administrative costs, overlapping controls and audits (for example, on risk management or incident response), and a reduced focus on actual security improvements within organisations.

**12. Position the sovereignty requirements within the appropriate European policy instruments and mechanisms.** When it comes to addressing concerns about the integrity or trustworthiness of certain supply chain actors, the ECCF is not the most appropriate vehicle to safeguard sovereignty with a view to unintended consequences. Including a potentially adverse impact on European competitiveness, the pace of innovation within the EU, and the integrity of the internal market. Furthermore, such requirements may complicate cooperation with strategically important economic partners. Embedding these requirements in the CSA-schemes themselves could lead to market distortion and risks undermining the level playing field among European companies. Therefore alternative approaches to address strategic risks such as sovereignty related concerns or other trustworthiness risks should be considered. This could be addressed:

- in the forthcoming Data Union Strategy or EU Cloud and AI Development Act, where broader data governance and resilience issues are more appropriately discussed; or
- be tackled through a separate, flexible EU-level mechanism, capable of adapting to evolving political and economic realities.

Such an **Evaluation Mechanism based on Trustworthiness** could take the form of a European trust evaluation framework focused on the supply chains of non-European providers and vendors. This mechanism would function as a precondition for market access and be based on a risk assessment of geopolitical, legal, and operational trustworthiness. Importantly, such an assessment on immunity requirements could operate in parallel to CSA certification schemes, allowing technical assurance and political risk screening to be addressed through distinct but complementary channels. It could entail both security and legislative criteria, including criteria on extra-territorial legislation and data transfers and GDPR compliance. The building blocks of this approach could be based on the strategic measures on risk profiles of the 5G toolbox. Such a mechanism could be considered to be incorporated in the larger framework of the CSA legislative proposal. However, it should be a separate evaluation mechanism from the cybersecurity certification framework which should remain focused on managing technical risks.

**13. Clarification of the role of Conformity Assessment Bodies (CABs) in third countries.** The CSA should provide greater clarity regarding the possibility for Conformity Assessment Bodies (CABs) to carry out certain testing activities—particularly in relation to the EUCC — outside the EU. It is recommended that CABs performing evaluations at the 'high' assurance level, giving preference to EU or EEA while taking into account the risk profiles of the country or region of the CAB.

## C. Cooperation with stakeholders and uptake of schemes

**14. Leverage the years of experience and expertise of existing standardization and certification institutions**. The value of a standard is realized only when this standard, developed by the community, is internationally embraced and adopted. For broad support and successful adoption, close collaboration between industry, associations, public administrations, academia, and societal organizations is crucial. A good example of the effectiveness is the Common criteria scheme that is based on international standards. It demonstrated that a close collaboration with the European Standardization Institutions is important to further underpin the implementation of EU cyber legislation. A procedure or coordination when starting to develop a scheme could create a common ground.

**15. Strengthen the role of the Stakeholder Cybersecurity Certification Group (SCCG)** to ensure private sector engagement in development and maintenance of schemes. This is essential for garnering sufficient support and fostering acceptance and uptake of the certification schemes by the market. The SCCG was established with the aim of institutionalizing this dialogue. However, the mandate of the SCCG has been found to be too limited with only being able to provide an opinion on the URWP. To enhance the relevance and practical impact of certification, the SCCG should be granted a more prominent and formalized role throughout the full lifecycle of certification schemes, including early-stage input, structured consultation during drafting, and regular feedback during implementation and review.

**16. Encouraging the Reuse of High-Quality Audit Reports**
To promote efficiency and reduce unnecessary costs for businesses, it would be beneficial for the framework to explicitly allow the reuse of high-quality audit reports. While ISO certification reports are a valuable resource, it is equally important to recognize other internationally accepted standards, such as those based on ISAE (International Standard on Assurance Engagements). The current exclusive reference to ISO 17065 may inadvertently suggest a limited scope for acceptable reports. Embracing a broader range of credible assurance frameworks would support diversity in assurance approaches while maintaining the integrity and reliability of assessments.

## Part 3. Simplification

**17. We support the Commission's effort of simplifying regulatory actions within the digital sector to reduce complexity.** A more coherent and aligned approach on digital legislation will on the long term foster the development of a uniform and effective framework for cybersecurity standards within the EU. It is, however, important to underline the fact that Member States are still in the process of implementing the different regulations, and that making changes at this stage will increase the workload of the already scarce cyber workforce. We therefore encourage the Commission to firstly investigate how streamlining the different legislations within the cybersecurity landscape can be effectuated, and whether the solutions proposed (aligning reporting templates, unification of time limits, harmonization of thresholds etc), will effectively lead to simplification and reduction of regulatory burdens. While some reporting obligations may easily be merged due to their common nature (e.g. NIS2 and CER directives), we see practical and legal challenges for other types of legislation (e.g. CRA and GDPR) where reporting frequency, purpose, mandate and responsibilities vary profoundly.

**18. We encourage the Commission to clearly identify both the challenges and advantages concerning the introduction of a Single Reporting Platform** before introducing this idea in new legislation. It is currently unclear whether the concept of a Single Reporting Platform on an EU and national level will effectively reduce the regulatory burdens for incident reporting. That could be investigated after a few years, when concrete data on incident reporting will be available.