



Position Paper on the European Parliament's Report for the Directive on the resilience of critical entities

Brussels, 10 November 2021

The Confederation of European Security Services (CoESS) highly welcomes the [report](#) of the European Parliament on the European Commission's [proposal](#) for a Directive on the resilience of critical entities (*in this paper referred to as "CER Directive"*). With this position paper, CoESS takes the opportunity to highlight those Amendments, which we believe should be adopted in interinstitutional negotiations.

On the whole, CoESS supports the Amendments tabled by the European Parliament, and congratulates the Members of European Parliament involved. We believe that the proposed additional provisions would substantially improve the quality of the legal text, enhance the resilience of critical entities (and hence the European internal market), better protect the public against existing and emerging security threats, and ensure higher coherence with the European Commission's proposal for a NIS Directive 2.

In particular, CoESS considers Amendments 25, 36, 37, 67, 76 and 81 in the European Parliament Report as highly important additions to the legal text. We recommend that they should be further supported by valuable Amendments previously proposed by the Opinions of the Parliament Committees on the Internal Market and Consumer Protection (IMCO) and Industry, Research and Energy (ITRE).

1. Recognition of Standards relevant for the protection of Critical Entities

CoESS highly welcomes the recognition of the added value of existing European Standards for the resilience of Critical Entities in the European Parliament's report - notably Amendment 76 establishing a new Article 13a on Standards.

This provision enhances coherence with the NIS Directive 2, notably the latter's Article 22, and was, without objective justification, missing from the original proposal for a CER Directive - despite clear recommendations from the European Parliament and although relevant European or internationally accepted standards exist that can serve enhanced resilience and physical protection of critical entities, as we outlined in detail in our [previous position paper](#).



Recommended approach: European Parliament Report, Amendments 36 and 37 establishing new Articles 2.1.7a and 2.1.7b, and Amendment 76 establishing a new Article 13a:

Article 2.1.7 (a) "standard" means standard as defined in Article 2, point (1), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council.

Article 2.1.7 (b) 'technical specification' means technical specification as defined in Article 2 point (4), of Regulation (EU) No 1025/2012;

Article 13a - Standards - In order to promote the consistent implementation of this Directive, Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of standards and specifications relevant to the security and resilience of critical entities.

To enhance coherence in the legal text, we further recommend the European Parliament Reports' Amendment 25 establishing Recital 27a on Standardisation:

Recommended approach: European Parliament Report, Amendment 25 establishing Recital 27a:

(27a) Standardisation should remain primarily a market-driven process. However, there might still be situations where it is appropriate to require compliance with specified standards at Union level. The Commission and the Member States should support and promote the development and implementation of standards and specifications relevant to the resilience of critical entities as set by the European Standardisation Organisations for the undertaking of technical and organisational measures aimed at ensuring critical entities' resilience. Member States should also encourage the use of internationally accepted standards and specifications relevant to resilience measures applicable to critical entities.

Standards can be particularly helpful for quality control of private security services: three European standards already exist, which list the quality criteria for security services suppliers for Aviation and Airport environments (EN16082:2011), for Maritime and Port environments (EN16747:2015), and for any type of Critical Infrastructure (EN17483-1:2021). These existing and future standards are a highly efficient way (1) to ensure the provision of qualitative private security services for CIP across Europe and (2) to support operators of critical entities in complying with the provisions of Article 11.



We therefore recommend the European Council to consider an amendment that was originally proposed by the European Parliament's Industry, Research and Energy Committee, which would effectively promote the use of Standards that are relevant for the resilience of Critical Entities:

[Recommended approach: ITRE Opinion, Amendment 30 establishing a new Article 11.1.da:](#)

Article 11.1(da) make use of accepted European standards and specifications relevant to the resilience of critical entities, without imposing the use of a particular type of service or technology or discriminating in favour of it;

2. Quality control of private security services in Critical Infrastructure Protection

CoESS highly welcomes Amendment 67 in Article 11 of the European Parliament Report in order to guarantee quality control and compliance of private security services protecting Critical Infrastructure.

[Recommended approach: European Parliament Report, Amendment 67 in Article 11.1e:](#)

*Article 11.1(e) (e) ensure adequate employee security management, including by setting out categories of personnel exercising critical functions, **laying down appropriate training requirements and qualifications**, establishing access rights to sensitive areas, facilities and other infrastructure, and to sensitive information as well as identifying specific categories of personnel in view of Article 12; **where external providers are involved in employee security management**, critical entities shall ensure that they comply with generally accepted standards and specifications.*

We believe however that the wording of this amendment can be improved as per the change tagged in yellow in order to provide legal clarity of the scope of this provision.

This Amendment was an important recommendation of our previous, [more detailed position paper](#), and are in line with Recital DV. of the [European Parliament's Report of the Special Committee on Terrorism](#), which states, with regard to the protection of Critical Infrastructure, that "*whereas private security services play a role in ensuring resilient security chains, public procurement of their services should therefore be subject to specific quality criteria, with regards to aspects such as the training, vetting and screening of personnel, quality control and compliance assurance, and the implementation of technological developments and contract management*".

3



3. Work of the Critical Entities Resilience Group and cooperation with external stakeholders, including private security services

CoESS is convinced, as explained in [our earlier, more detailed position paper](#), that cooperation with third parties and private stakeholders involved in Critical Infrastructure Protection, such as private security services, is key.

We therefore strongly support Amendment 81 of the European Parliament Report within Article 16.2.1.

Recommended approach: European Parliament Report, Amendment 81 within Article 16:

*Article 16.2.1: The Critical Entities Resilience Group shall be composed of representatives of the Member States and the Commission. Where relevant for the performance of its tasks, the Critical Entities Resilience Group shall invite representatives of relevant stakeholders, **such as representatives of European professional associations, associations of critical entities, critical entities of particular European significance, industry and research centres relevant for each focused economic sector** to participate in its work and the European Parliament to participate as an observer.*

We believe however that the wording of this amendment can be improved as per the change tagged in yellow in order to provide legal clarity of the scope of stakeholder covered by this provision.

We further recommend to add a provision to Article 16.3, which ensures adequate guidance to operators of Critical Entities on useful Standards that can serve their better protection.

A vast range of European Standards exists, which often lack promotion among relevant stakeholders. An amendment which was originally proposed by the Opinion of the European Parliament's Committee on Internal Market and Consumer Protection would therefore be useful to be considered :

Recommended approach: IMCO Opinion, Amendment 121 establishing a new Article 16.3hc:

Article 16.3(hc) exchanging best practices and information on all other matters in relation to the implementation of this Directive, including the application and development of standards and technical specifications;

About private security services for the protection of critical infrastructure

The ways in which Critical Infrastructures are currently secured and protected vary in the European countries from a mixture of state authorities (police, specialist protective services and occasionally the military), in-house private security officers, to fully contracted out to private security companies. Private security companies provide a wide range of guarding and surveillance services for all kinds of Critical Infrastructures - including for example nuclear plants, water supply systems, government buildings, healthcare facilities, maritime ports, aviation / airports and other public transport means and hubs. It is undoubtedly a development in Europe that the CIP tasks are increasingly contracted out to the private security sector. Private security services therefore play a crucial role in the security supply chain to enhance resilience of Critical Infrastructures as defined in Article 2 of the proposal for CER Directive. Due to this trend, it is a prerequisite of enhanced resilience that private security services comply with the highest quality standards.

About CoESS

CoESS acts as the voice of the private security industry, covering 23 countries in Europe and representing 2 million security officers as well as over 45,000 companies. The private security services provide a wide range of services, both for private and public clients, ranging from Critical Infrastructure facilities to public spaces, supply chains and government facilities. CoESS is recognised by the European Commission as the only European employers' organisation representative of the private security services. Representing a labour-intensive sector, CoESS is actively involved in European Sectoral Social Dialogue and multiple EU Expert Groups - including SAGAS, SAGMAS, LANDSEC, RAILSEC and the EU Operators Forum for the Protection of Public Spaces.

EU Transparency Register Number: 61991787780-18