Position Paper
on the European Commission's Proposal for a Directive on the resilience of critical entities

Brussels, 23 March 2021

The Confederation of European Security Services (CoESS) welcomes the European Commission's proposal for a Directive on the resilience of critical entities (*in this paper referred to as "CER Directive"*) and strongly supports most of its provisions. Following the Evaluation of Directive 2008/114 (SWD (2019) 308), CoESS called, in January 2020, for a revision of the Directive on the Identification of European Critical Infrastructures. Its repeal in form of the CER Directive, together with the European Commission's proposal for a NIS Directive 2, and the provision of cybersecurity and physical protection risk management measures of critical entities, is a highly important step for enhanced Critical Infrastructure Protection (CIP) in Europe and better resilience of critical entities against manifold, current and emerging, threats.

Still, CoESS believes that the European Commission's proposal for a CER Directive needs to go further to reach its objective to reduce vulnerabilities and enhance the resilience of critical entities by correcting two important deficiencies, namely:

1. **Take on board key recommendations of the European Parliament's Report of the Special Committee on Terrorism concerning the protection of Critical Infrastructure;**
2. **Align the European Commission's proposal with the proposal for a NIS Directive 2 on important matters where, without objective justifications, this is currently not the case.**

In this paper, we make a number of proposals to this end and call upon the European Parliament and Council to amend the European Commission's proposal for a CER Directive in the following matters:

- **Re-assess the Directive's scope;**
- **Align resilience measures in Article 11 with respective provisions of the NIS Directive 2;**
- **Include adequate provisions to put in place Insider Threat prevention policies;**
- **Recognise European and International Standards relevant to the physical protection of critical entities, as is the case in the NIS Directive 2.**

This position paper is divided in two parts: the detailed substantiation of the proposed changes (first part) and the concrete proposals for the amendments (Annex).

1. Re-assessment of the Directive's scope

CoESS welcomes that the CER Directive has a broader scope than Directive 2008/114 – taking into account different sectors of critical entities that are vital for the functioning of our societies and economies or at which an incident could have significant disruptive effects.

We also highly welcome that the European Commission's proposal for a CER Directive aims for close alignment with the proposal for a NIS Directive 2. Recital 8 correctly states that "***a coherent approach between this Directive and the NIS Directive 2 is necessary wherever possible***". At the same time, CoESS notes that the NIS Directive 2 covers, without objective justification, more sectors than the CER Directive – for example:

- Postal and courier services;
- Waste management;
- Manufacture, production and distribution of chemicals;
- Food production, processing and distribution;
- Manufacturing (e.g. military vehicles and medical devices).

CoESS therefore recommends to re-assess the proposal's scope based on risks that can be associated with disruptive incidents in different sectors.

We add that most of these sectors are recognised as Critical Infrastructure in a number of EU Member States[1] and/or in the USA[2], and remind lawmakers of the proposal's Specific Objective 2 to "***ensure that all relevant entities in all key sectors are identified as critical by Member States authorities***".

2. Alignment of resilience measures (Art. 11) with provisions of the NIS Directive 2

CoESS strongly supports the reasoning for the legal basis (Article 114 TFEU) of the European Commission's proposal for a CER Directive and welcomes that Article 11, as part of Chapter III of the proposal, includes physical protection and resilience measures for entities that have been identified

[1] European Commission Staff Working Document SWD/2020/368 final: Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities
[2] https://www.cisa.gov/critical-infrastructure-sectors

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **www.coess.eu**

as critical as per Articles 4 to 6. In this sense, we strongly support the Specific Objective 3 of the proposal to "***ensure that the full spectrum of resilience activities is included in public policies and operational practice***". Security and safety must thereby be seen as an enabler of the functioning of Critical Infrastructure.

We also welcome that Recital 8 rightly states that "***a coherent approach between this Directive and the NIS Directive 2 is necessary wherever possible***". This is in line with the call of the EU Security Union Strategy, which states that "***false distinctions between the physical and digital need to be overcome***".

CoESS strongly agrees with these statements. Robust physical and cybersecurity cannot be envisaged separately from each other without risk of compromising them both. Security professionals even go further and argue that this silo reasoning in itself is a source of vulnerabilities. It is well known that most cyber attacks can only happen with a human intervention, voluntary or involuntary. A breach in physical protection can lead to a serious cybersecurity incident – for example in access control to IT equipment and control rooms at critical entities. Conversely, a cyber attack can compromise or destroy physical assets. Neither can be effective without the other.

Due to this interdependence between physical protection and cybersecurity, also the European Parliament's Report of the Special Committee on Terrorism "***calls for Directive 2008/114 to be revised in order to provide similar rules and procedures for 'operators of essential services' as in the NIS Directive***" in recommendation 174.

Unfortunately, we note that this is not the case - despite what the European Commission emphasises in Recital 8: Article 11 of the CER Directive falls short of the provisions made in Article 18 of the proposal for a NIS Directive 2 (see box on the right). In contrast to the NIS Directive 2, the CER Directive does not include provisions on supply chain security and quality control of suppliers and service providers. CoESS does not see any objective justification why such

Articles 18.2 and 18.3 on "Cybersecurity risk management measures" of the NIS Directive 2 proposal rightly oblige critical entities to take measures that include:

*18.2(d) **supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers** such as providers of data storage and processing services or managed security services;*

*18.3 Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities shall take into account the **vulnerabilities specific to each supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers**, including their secure development procedures.*

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | catherine@coess.eu | www.coess.eu

provisions should apply for cybersecurity risk management measures and not physical resilience measures of critical entities, so this should be corrected in Article 11 of the CER Directive.

As the representative of the European private security services, CoESS feels very concerned by matters of quality control and supply chain security, and strongly recommends that such amendments to Article 11, as outlined in the Annex of this paper, should include provisions concerning security services that are outsourced for the protection of critical entities.

Private security provides an essential service in Critical Infrastructure Protection (CIP), which has also been recognised by the European Commission[3] as a critical occupation during the COVID-19 pandemic. Our recommendation is also 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 regard 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***".

CoESS strongly calls on the European Parliament and Council to follow this recommendation and add the provisions on risk management measures in supply chain security and quality control, which are already included in Article 18 of the NIS Directive 2, to Article 11 of the CER Directive. In line with the abovementioned Report of the European Parliament's Special Committee on Terrorism and as part of necessary quality control, we also recommend to include additional provisions for operators of critical entities to ensure:

- **compliance of security services with applicable training requirements, as laid out in national and/or European legislation;**
- **that when outsourcing security services, quality criteria prevail costs in a 60/40 ratio.**

Our proposals for concrete amendments in the text are outlined in the Annex of this paper.

CoESS underlines that shortcomings in quality control of security services can be a serious vulnerability to CIP. When qualitative criteria, e.g. related to training and working conditions of security staff are

[3] Communication from the European Commission: Guidelines concerning the exercise of the free movement of workers during COVID-19 outbreak (2020/C 102 I/03).

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | catherine@coess.eu | www.coess.eu

not met, this can lead to very serious security gaps, as well as risks to public safety and security, let alone the critical entities' performance itself. The respect of quality in security services is not only part of a global understanding of resilience, but an enabler for the functioning of Critical Infrastructure and services that are essential for society. We stress that qualitative security services are in the public interest, particularly when they protect Critical Infrastructure and/or work in collaboration with public forces. Compromises on quality in matters of security may have serious consequences and must be excluded: low-cost focused procurement that ignores important quality criteria provides incentives for non-compliance with legislation, including labour law, collective bargaining, hiring inadequately qualified, trained and vetted security personnel, and compromised contract performances, which in turn lead to lower security. At our societies' most important infrastructures, such a cost vs. quality (instead of best value) attitude and related vulnerabilities can lead to severe consequences. To enhance the resilience of critical entities, the CER Directive must reduce such vulnerabilities.

In Spain, for example, national law foresees that quality criteria must represent at least 51% in the awarding process of all private security services. CoESS believes that for the protection and resilience of critical entities, this threshold should be even higher, at 60% (60/40 ratio against costs). The Guide "Buying Quality Private Security Services", co-produced by CoESS and its Social Partner UNI Europa with EU funding (available at www.securebestvalue.org), provides important and concrete guidelines for the definition of quality criteria in private security services in CIP in compliance with Directive 2014/24/EU on public procurement. As Directive 2014/24/EU only applies to public operators of critical entities, CoESS strongly recommends that lawmakers in European Council and Parliament ensure that the CER Directive establishes a level-playing field between both public and private operators of critical entities in the internal market when it comes to quality control in procurement and outsourcing of security services.

The advisory missions mentioned in Article 11.3 of the proposal should be able to provide advice to public and private operators of critical entities on how to meet such obligations. Furthermore, CoESS recommends adding to the tasks of the Critical Entities Resilience Group in Article 16.3 to "support Member States and critical entities in meeting obligations referred to in Chapter III by means of best practice and information exchange as well as non-binding guidance documents".

3. Inclusion of adequate provisions on Insider Threat Frameworks

The reasons and objectives of the European Commission's proposal rightly mention Insider Threats as part of the complex risk landscape that operators of critical entities are dealing with today. Recital 24 further clarifies that "*The risk of employees of critical entities misusing for*

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **www.coess.eu**

***instance their access rights within the entity's organisation to harm and cause damage is of increasing concern*". Recital 2 adds that entities operating Critical Infrastructures "*are not adequately equipped to address current and anticipated future risks to their operations*".**

It is therefore necessary to include provisions in the CER Directive to make sure that operators of, and the whole ecosystem around, the critical entities have Insider Threat detection and protection policies in place. Both cyber and physical Insider Threats can cause severe damage physically, financially and to reputation, whatever the underlying objective may be (crime, espionage or terrorism) and whether it is caused intentionally, by negligence or just as a result of a lack of awareness. CoESS believes that provisions on "adequate employee security management" in Article 11.1.e and on "background checks" in Article 12 are important and a step in the right direction, but are not explicit enough and are insufficient to adequately address the challenge of Insider Threats. A policy to counter Insider Threats must, among others, include a continuous screening of employees, not just one-off actions like vetting and screening, and need to also cover risk assessment and mitigation of critical assets with a focus on risks from Insiders. What is more, Insider Threat policies must include several departments in order to create a team that can prevent, mitigate and enquire. This includes HR, IT and Finance, mainly, with a clear endorsement from top management.

We therefore recommend including the provision to set in place an Insider Threat policy as part of Article 11.1 of the CER Directive. Our proposals for concrete amendments in the text are outlined in the Annex of this paper.

As mentioned above, CoESS recommends adding to the tasks of the Critical Entities Resilience Group in Article 16 to "support Member States and critical entities in meeting obligations referred to in Chapter III by means of best practice and information exchange as well as non-binding guidance documents".

CoESS takes the opportunity to raise awareness of the deliverables of the EU-funded AITRAP project, i.e. an eLearning platform and set of tools and guidelines on how to detect and protect against Insider Threats in Critical Infrastructure. Co-funded by the Internal Security Fund of the European Union, Help2Protect.info is an online platform hosting two sets of eLearning tools: an Awareness Training and an Insider Threat Program Builder. The target audience is all types of Critical Infrastructure. The ultimate goal of Help2Protect is to engage all stakeholders to protect themselves, their colleagues, their company and the infrastructure they work for against Insider Threats. CoESS has also introduced many findings of the project in the guidance document on "Good Practices in Combatting Insider Threats in the Rail Sector", developed within the EU Rail Passenger Security Platform (RAILSEC) which is mentioned in the proposal's Recital 23.

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **www.coess.eu**

4. Recognition of European and International Standards relevant for the physical protection of critical entities

Article 22 of the proposal for a NIS Directive 2 includes highly important recommendations for the use of European and International standards in order to fulfil mandatory cybersecurity risk management measures (see box on the right). Such provisions are, for no objective reason, missing from the European Commission's 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, such as on information security management (ISO/IEC 27000:2018), on security management systems for the supply chain (ISO 28000:2007), and multiple European standards for security services (EN16082:2011; EN16747:2015), including those that are outsourced for the protection of Critical Infrastructure (FprEN17483-1). Moreover, Recommendation 176 of the European Parliament's Report of the Special Committee on Terrorism, referring to the protection of Critical Infrastructures, calls "*on the Commission to propose a European Certification Initiative for private security companies, aiming to specify the requirements and conditions under which they can operate within the critical infrastructure environment*".

Article 22 of the NIS Directive 2 includes following provisions concerning Standardisation:

22.1 In order to promote the convergent implementation of Article 18(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.

22.2 ENISA, in collaboration with Member States, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standard, which would allow for those areas to be covered.

CoESS therefore calls on the European Parliament and Council to consider this recommendation and add Article 22 on "Standardisation" of the NIS Directive 2 to the CER Directive. Our proposals for concrete amendments in the text are outlined in the Annex of this paper.

The Critical Entities Resilience Group, to be established by the European Commission's proposal, could draw up advice and guidelines regarding the Standards and areas to be considered in relation to this provision – similar to the role that is foreseen to ENISA in the NIS Directive 2 proposal.

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | catherine@coess.eu | www.coess.eu

Such Standards can be particularly helpful for quality control of private security services. Whilst two European standards already exist, which list the quality criteria for security services suppliers for Aviation and Airport environments (EN16082:2011) and for Maritime and Port environments (EN16747:2015), the CEN Technical Committee (TC) 439 "Private Security Services" has already adopted a General Requirements standard for security services supplied in any type of Critical Infrastructure (FprEN17483-1), which is awaiting publication 2021 Q2. The above-mentioned aviation and maritime standards are being revised as additional sector-specific branches of the future EN17483 Standard System, as prEN17483-2 and 17483-3, respectively. In the future, the TC intends to address other Critical Infrastructure sectors, such as energy, healthcare/hospitals and water supply as further "branches" of the above standard system.

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) support operators of critical entities in complying with the provisions of Article 11. They are designed by specialists from the industry and are therefore credible and widely approved means to specify service requirements for quality in organisation, processes, personnel (incl. training and vetting), Insider Threat policies and management of a security service provider.

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **www.coess.eu**

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 are therefore playing a crucial role in the security supply chain to enhance resilience of Critical Infrastructures as defined in Article 2 of the proposal for a Directive on the resilience of critical entities. 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

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **www.coess.eu**

ANNEX

SUGGESTIONS FOR AMENDMENTS TO THE EUROPEAN COMMISSION'S PROPOSAL FOR A DIRECTIVE ON THE RESILIENCE OF CRITICAL ENTITIES

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **www.coess.eu**

1. Alignment of resilience measures (Art. 11) with provisions of the NIS Directive 2

2. Inclusion of adequate provisions on Insider Threat Frameworks

Suggested amendment to Article 11
11.1 Member States shall ensure that critical entities take appropriate and proportionate technical and organisational measures to ensure their resilience, including measures necessary to: (a) prevent incidents from occurring, including through disaster risk reduction and climate adaptation measures; (b) ensure adequate physical protection of sensitive areas, facilities and other infrastructure, including fencing, barriers, perimeter monitoring tools and routines, as well as detection equipment and access controls; (c) resist and mitigate the consequences of incidents, including the implementation of risk and crisis management procedures and protocols and alert routines; (d) recover from incidents, including business continuity measures and the identification of alternative supply chains; (e) ensure adequate employee security management, including by setting out categories of personnel exercising critical functions, 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; ~~(f) raise awareness about the measures referred to in points (a) to (e) among relevant personnel;~~ (f) ensure that an Insider Threat detection and prevention policy is put in place; (g) ensure supply chain security including security-related aspects concerning the relationships between each entity and its service providers such as security services; (h) ensure compliance with applicable training requirements among relevant security personnel as laid out in national and/or European legislation; (i) raise awareness about the measures referred to in points (a) to (h) among relevant personnel. 11.[new] Member States shall ensure that, where considering appropriate measures referred to in points (a) to (h) of paragraph 1, entities shall take into account the overall quality of products and service practices of their security service providers. When outsourcing security services, quality criteria shall prevail over costs in a 60/40 ratio. Compliance of security service providers with relevant national sectoral and labour law must at all times be guaranteed and proven.

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | catherine@coess.eu | www.coess.eu

Suggested amendment to Article 16
16.3 (new) support Member States and critical entities in meeting obligations referred to in Chapter III by means of best practice and information exchange as well as non-binding guidance documents.

3. Recognition of European and International Standards relevant for the physical protection of critical entities

Suggested introduction of a new Article on Standardisation as part of Chapter III
NEW Article Standardisation 1. In order to promote the convergent implementation of Article 11(1) and 11.[new], Member States shall, without imposing or discriminating in favour of the use of a particular type of service or technology, make use of European or internationally accepted standards and specifications relevant to the resilience of critical entities. 2. The Critical Entities Resilience Group shall draw up advice and guidelines regarding the areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered.

Suggested amendment to Article 16
16.3 (new) draw up advice and guidelines in support of Article [NEW ARTICLE ON STANDARDISATION AS PART OF CHAPTER III].

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Avenue des Arts | Kunstlaan 56 | B-1000 Brussels | Belgium
Mobile : +32 472 180 107 | catherine@coess.eu | www.coess.eu