Position Paper

Confederation of European Security Services

Comments on the

Draft Commission Non-Paper « Good Practices to support the protection of public spaces »

We are grateful for the opportunity to comment on this document, discussed at the Operators Forum on the Protection of Public Spaces on 26 November 2018, and which serves as an excellent basis for discussion. The comments also cover interventions made during the meeting.

The following comments are meant to contribute positively to the further development stage of the document.

General comments

Integrated security: CoESS strongly supports the principle, whereby security needs to be integrated in the design and management of public places, much in the same way as safety has been. There are synergies between security and safety, which should be explored. In response to a comment made by one of the MS representatives on the cost of security, CoESS would like to highlight that this is possibly much lower than the cost of a security incident. Safety also entails cost, but no one today would question the legitimacy of safety measures. Due to the synergies between security and safety, their integration into the design and management of public spaces would reduce cost of implementing a separate security measure.

Terminology: it would be helpful to refer to existing definitions, either European or International, for concepts such as risk, crisis, vulnerability, and threat. The ISO Terminology standard on Societal Security (22300:2018) may be helpful in this respect.

Processes: it may also be useful to refer to ISO documents on Risk Assessment (ISO 31000 series) and Supply Chain Security (ISO 28000 series). This would meet the need of following the same methodology.

On-going standardisation work: ISO TC292 "Security and Resilience" and, in particular, its WG6 "Protective Security" are developing standards that could be useful for operators, which are not

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **coess.org**

necessarily very familiar with security. The current projects look at creating a protective security architecture and how to make a security plan. CoESS offers to report about the TC 292 WG6 activities and to liaise with their experts, if at any time this would become of interest to DG HOME and/or the Operators' Forum.

The role of Private Security Companies: CoESS welcomes the special role given to private security, as part of the "security continuum", and wishes to support the forum with expertise and documents, e.g. the Best Practice document on Transport Security. This document can be found here: http://coess.org/newsroom.php?page=position-papers (3rd document from the top).

Quality of Private Security Services: CoESS and its members highlight that Private Security Companies can only play their role effectively if the selection criteria are quality and not the lowest cost. Operators may wish to outsource security and, in this case, should make sure that they are buying services based on quality criteria, and not just cost. The EU-funded guide, which CoESS developed jointly with UNI Europa, can be found at the following link in 14 languages: www.securebestvalue.org. The Best Value Guide takes buyers through the quality criteria that ought to be checked when buying security services.

The Private Security Guards, which in the EU are about 1.5 million, i.e. about the same number of police officers, could be better used – if trained to this effect – to help detect unusual behaviours or activities. As they are located in multiple public, private and semi-public spaces, they could be the eyes and ears of law enforcement. A number of projects are in place across Europe in order to optimise this untapped potential.

Going through the recommendations in a detailed way (titles are those of the Commission document, followed by the comments of CoESS):

1. Vulnerability assessment:
    a. The paper indicates that operators should carry out vulnerability assessments. It is important that this be done based on a common methodology tool and that operators have the capacity to carry out such assessments. It is therefore very useful to have an EU vulnerability assessment tool. Private Security Companies can also assist operators in carrying out vulnerability, risk and threat assessments.
2. Security by design
    a. CoESS supports the concept of security by design. However, this concept should not address one building or facility only, but also the facilities around and the whole urban planning, and how response can be organised in an integrated way.

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **coess.org**

b. In the work done by ISO TC 292 to address security in a holistic way, there is also ongoing work on security by design. It may be interesting for DG HOME to get a general overview of the work being done at ISO level.

3. Develop and implement a facility or event security plan
    a. Preparing a security plan, analysing the threat, assessing the vulnerabilities, evaluating the security "appetite", these are tasks that need to be performed by professionals, either within the company or outsourced. Not all operators have a security specialist and Private Security Companies are there to provide such services to companies.
4. Appoint and train a person responsible for the coordination and implementation of security measures contained in the security plan -
   As indicated above, not all companies have the size and resources to have a dedicated person, let alone a team, to handle security in a professional way. Therefore, this person may be outsourced to specialised companies.
5. Develop and implement an internal security awareness programme for all employees – CoESS very much supports this kind of awareness programme, as security is everybody's concern, not just the person in charge of security.
6. Develop and implement a crisis communication plan
    a. The communication plan should be part of the crisis management plan, which should determine also who should be part of the crisis management team, and who should be the spokesperson in case of a crisis.
7. Assess the necessary access controls and barriers
    a. In order to avoid creating new vulnerabilities and bottlenecks, it is important that the security measures be considered as a dynamic, so-called "security solutions" process. For example, when ordering security, the client should not himself determine how many guards are needed at the entrance, but rather indicate the number of people who enter the building at any one time, with peak hours, etc. Only in this way can the measures be tailored to the needs. A counter-example of this is the access to Centre Borschette, where there are regular 20-minute queues on the pavement, because the exact same number of guards are present no matter the hour or number of visitors, although with the registration system, the Conference Centre knows with a high level of precision how many visitors will arrive at what time.
8. Assess the most appropriate detection technology
    a. This is also a matter that should be discussed with security providers, as operators are not necessarily aware of recent or emerging threats, and it is not their business to research this kind of matter.

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **coess.org**

9. Develop basis security training programmes
    a. CoESS supports better education in terms of security, as security providers can do a better job with customers who are aware of the needs and requirements to ensure proper and high-quality security services. For this to happen, it is important to ensure a consistent and high level of quality in security training. This can be ensured by establishing curriculum requirements and quality standards.
10. Develop and implement internal insider threats awareness programme
    a. The AITRAP project, with its online awareness training programme at www.Help2Protect.eu, is timely and can meet this need. Solutions to translate the awareness training are being sought, and the help from the Commission would be very welcome in this sense. The cost is not very high, since the programme already exists and has been tailored to a very wide public.
11. Undertake regular security exercises
    a. CoESS supports this principle and would like to add that the security exercises should be designed according to a PDCA (Plan Do Check Act) principle. They should be evaluated and the outcome of the evaluation should be used to improve the response to attacks.
12. Develop and share guidance materials with other operators of the same industry branch.
    a. CoESS supports the exchange of experience and guidance materials and would suggest that this can be broadened to other industry branches.

Public authorities as well as operators should consider to:

1. Appoint contact points and clarify respective roles and responsibilities in public-private cooperation on security matters and for a better communication and cooperation on a daily basis.
   CoESS strongly supports this principle, as it is one of the points that it makes in its document on Best Practices in Transport Security. At present, PSCs become informed of security events at the same time as the general public, although their guards are first in line responders, as has been shown in the recent terrorist attacks. It is also in the authorities' best interest that security companies are kept in the communication loop in emergency situations, so that they can prepare and respond, and come in support of public emergency response services.
2. Establish trustful communication and cooperation that allows for a useful risk and threat information exchange between responsible public authorities, local law enforcement and private operators.

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **coess.org**

a. CoESS fully supports multi-stakeholder cooperation and, to this end, points to the experience of countries where this cooperation exists and is effective. CoESS has gathered some examples of effective PPP in the Netherlands, the UK and Norway and will in the near future start writing a White Paper on PPPs.

Public authorities should consider to:

1. Coordinate the work on protection of public spaces
2. Initiate public awareness campaigns on reporting of suspicious behaviour
3. Make available practical recommendations to operators to detect, mitigate or respond to security threats.

CoESS fully supports these points, but emphasises that operators are not, and should not become, security specialists. It is important to identify specific roles and responsibilities of each type of stakeholder: public, private operators, security services providers, citizens, media, etc.

Private Security Companies have specific knowledge, experience and expertise, and can play an active role in this chain.

Brussels, 5 December 2018

Catherine PIANA, Director General
CoESS | Confederation of European Security Services
Jan Bogemansstraat | rue Jan Bogemans 249 | B-1780 Wemmel Belgium
Mobile : +32 472 180 107 | **catherine@coess.eu** | **coess.org**