Council of the European Union

Brussels, 25 March 2019
(OR. en)

7434/19
ADD 2

JAI 331
COSI 57
FRONT 120
ASIM 38
DAPIX 117
ENFOPOL 122
SIRIS 57
VISA 70
FAUXDOC 26
COPEN 128
CYBER 105
DATAPROTECT 108
CT 29
JAIEX 49
EF 124

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	21 March 2019
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2019) 140 final
Subject:	COMMISSION STAFF WORKING DOCUMENT Good practices to support the protection of public spaces Accompanying the document Communication from the Commission to the European Parliament, the European Council and the Council Eighteenth Progress Report towards an effective and genuine Security Union

Delegations will find attached document SWD(2019) 140 final.

Encl.: SWD(2019) 140 final

EUROPEAN
COMMISSION

Brussels, 20.3.2019
SWD(2019) 140 final

COMMISSION STAFF WORKING DOCUMENT

Good practices to support the protection of public spaces

Accompanying the document

Communication from the Commission to the European Parliament, the European Council and the Council

Eighteenth Progress Report towards an effective and genuine Security Union

{COM(2019) 145 final}

Introduction

Recent terrorist attacks have shown a recurrent targeting of public spaces, exploiting the intrinsic vulnerabilities that result from their open nature and public character. To address these threats and enhance the protection of public spaces, the European Commission adopted in October 2017 an EU Action Plan[1], aimed at supporting EU Member States through funding, the exchange of good practices and lessons learnt, establishing and facilitating networks, enhancing cooperation and providing guidance material.

In December 2017, the Commission launched a public-private Operators Forum bringing together Member States' policy makers and operators from different sectors, such as mass events and entertainment, hospitality, shopping malls, sports and cultural venues, transport hubs and others. A first meeting of the Forum took place on 20 December 2017, with all sectors represented. Subsequently, the Commission organised thematic subgroup meetings in December 2017, June and September 2018 focusing on car rentals, mass events/ entertainment, transport, hospitality and commerce sectors.

The meetings made evident that many public authorities and operators have already launched initiatives to strengthen the security of their venues. Good practice materials have been shared with the Commission, who has made it available to participants of the Operators' Forum via its dedicated CIRCABC platform, serving as the main repository for materials and information.

The meetings have also shown remaining challenges and gaps. Protection levels are very uneven across the various sectors, and even within the same sectors important differences have been noted. While some sectors have a well-developed security culture, others are only now putting in place more systematic approaches to protecting their venues. To develop of a common culture of security is key. It needs to be shared between public authorities, private actors and citizens.

Drawing on the discussions and material provided within the public-private Operators Forum, good practices were identified for operators and public authorities to strengthen the security of public spaces.

At the second meeting of the Operators' Forum on 26 November 2018, participants were invited to discuss these good practices and to make suggestions to further improve them. Participants were also encouraged to exchange on ways for different sectors to use these good practices to enhance the security of their public spaces. The consultation process further included representatives of Member States in an EU Council working group and Commission services.

[1] COM(2017) 612 final (18.10.2017).

Context

The formulation of the good practices has also benefited from a number of other activities that have been pursued over the last 15 months.

In March 2018, the Commission and the Committee of the Regions organised the EU Mayors' conference on "Building urban defences against terrorism: lessons learned from recent attacks". The conference, which gathered close to 200 participants, focused on lessons learned from recent terrorist attacks, sharing of experiences and good practices to enhance the physical protection of public spaces while maintaining the openness and attractiveness of cities and public spaces. A strong call to continue the exchange of information and cooperation with and among the local and regional level was voiced.

One follow-up from the conference was the creation of a new Partnership for Security in Public Spaces under the EU Urban Agenda[2], co-coordinated by the cities of Nice and Madrid together with the European Forum for Urban Security. It involves 14 partners from cities and national authorities of nine Member States, as well as several Directorate-Generals of the Commission. The aim is to develop and implement an Action Plan with concrete measures on how to enhance the security of public spaces in cities, such as the use of technology, urban planning and design, and sharing and managing public spaces.

EU funding to better protect public spaces has also been made available. The Commission published a call for proposals under the Internal Security Fund – Police for protection of public spaces and critical infrastructure against terrorist threats, worth over EUR 25 million in 2017. 15 projects were selected, of which seven focus on the protection of public spaces. Another call for proposals was published in October 2018 under the Internal Security Fund - Police with a budget of EUR 9.5 million. It focused inter alia on public-private cooperation in the protection of public spaces. In addition, the Commission published a call for proposals with a budget of EUR 100 million in October 2018 under the Urban Innovative Actions initiative as part of the European Regional Development Fund to provide cities with innovative solutions to address urban challenges. Urban security was one of the four priorities of this call. Both the Urban Innovative Actions call and the Internal Security Fund - Police call are closed. A new call under Horizon 2020 security research is addressing the protection of public spaces[3].

Moreover, the Commission organised a technical workshop with local authorities, urban planners and researchers in June 2018 at the Joint Research Centre focusing on technical issues regarding physical protection and in particular, the protection of city centres against vehicle ramming. A guideline for the selection of appropriate anti-ramming vehicle barrier systems is finalised and a training programme will take place in June 2019.

The Commission developed different guidance materials and compiled available guidance in the area of protection of public spaces. The operationalisation of the good practices collected in this document builds upon all available material.

---

2 https://ec.europa.eu/futurium/en/urban-agenda/terms/all/Security%20in%20public%20spaces.

3 Work programme: http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-security_en.pdf , Call ID: H2020-SU-INFRA-2018-2019-2020.

Good practices identified

The following good practices have been identified to improve the protection of public spaces. They are the result of an extensive consultation process and should serve as reference for operators and public authorities that wish to take further steps to protect public spaces.

Section 1: Assessment and planning

1. Establish and undertake **vulnerability assessments** to identify potential vulnerabilities against attacks by outsiders or insiders.

Operators should regularly carry out vulnerability assessments with respect to current and emerging threats to their facilities, in cooperation with law enforcement authorities. They should cross-check vulnerabilities and threats coming from the outside or inside, such as terrorist attacks, their direct and indirect consequences, for example a mass panic. An EU vulnerability assessment tool has been developed which can be used for this purpose. The vulnerability assessment is also often useful to protect against criminal offences.

2. Develop and implement a **facility or event security plan**, including preparatory, emergency and recovery measures, identifying the appropriate security measures for the facility's or event's environment. Security measures need to be effective, discreet, proportionate and tailor made for different environments, taking into account their specific functioning.

Every facility or event is unique and there is no one-size-fits-all solution. The operators should take into account the specific threat landscape, possible vulnerabilities and the nature of their facility or event to design a proportionate security plan fit for purpose. Selected tailor-made security measures need to be accompanied by appropriate technical solutions and to be performed by security experts, either within the company or outsourced.

3. **Appoint and train a person** responsible for the coordination and implementation of security measures contained in the security plan.

Public and private operators should appoint a competent person, as well as a backup, who understands the threats landscape and knows well the facility/event and make sure that this person receives the appropriate training.

4. Develop and implement a **crisis management plan**.

To ensure efficient management and communication in crisis situations with staff and customers, as well as with law enforcement, operators should prepare a plan (to alert, confine and/or evacuate), identifying a crisis communication team or a spokesperson and key messages. Modern technology such as smartphone applications can help facilitate communication with staff in emergency situations. In the technological assessment, the quality of the communication service, security of information transferred, the multimedia information service availability and the integration with automated emergency procedure should be taken into consideration.

Section 2: Awareness and training

1. Initiate **public awareness campaigns** on reporting of suspicious behaviour and how to react in the case of an attack compromising the security of a facility or event.

Any public awareness campaign should clearly state how to identify and report and who to contact in case of any suspicious behaviour or incident. It is also important to provide feedback to those reporting whether it is the public or operator

2. Develop and implement an internal **security awareness programme** for all employees.

Operators should consider issuing and visibly displaying posters, leaflets, and brochures containing information raising security awareness. Expertise of public authorities, especially law enforcement, should be taken into account.

3. Develop and implement an internal **insider threats awareness programme** that will help protect facilities or events against different types of insider threats, such as sabotage, commercial theft, or terrorist attacks.

Based on the vulnerability assessment, and in close cooperation with law enforcement authorities, operators should consider background checks and possible vetting of the staff in respect of national laws both before and during their assignments. The EU-funded AITRAP project[4] *with its online training programme is a good example for such a tool.*

4. Develop basic **security training programmes** for all staff and undertake specific security trainings, contributing to the development of a corporate security culture. Develop activities that motivate employees to implement sound security practices and keep a high level of security vigilance.

Staff working at the facility or event should be properly trained and regularly re-trained for the tools they operate. All members of staff should be aware of their responsibilities and role within the internal security structure. Regular trainings and simulations of possible threat scenarios can ensure smooth coordination but also help identify possible shortcomings. This is also to avoid creating new vulnerabilities and a false sense of security. Some of the trainings, namely the refreshing ones, could be covered by e-learning. The staff should also be trained on how to behave in unexpected situations, such as forced lockdowns.

5. Undertake regular **security exercises** that will help to identify the level of preparedness to deter and respond to an attack.

Operators should liaise with their local and, where appropriate, regional or national law enforcement and emergency services to design and train responses to possible threat scenarios. These should be regularly tested in table-top or real exercises in order to detect shortcomings and to tackle issues related to timely and proper response as well as task division. Exercises should involve all relevant stakeholders (e.g. rescue services, fire department, special forces and other relevant service providers), to ensure that the different plans fit each other and should be designed according to the "plan-do-check-act" principle and be evaluated.

[4] www.help2protect.eu

Operators should also have available and share their most up-to-date blueprints and premises information and maps with law enforcement agencies and emergency services so that appropriate response is ensured if needed.

Section 3: Physical protection

1. **Assess security and physical protection issues** from the beginning of the design process of a new facility or event.

Resilient structures, facilities and events can help to protect against multiple threats, and mitigate impacts. The so-called security-by-design concept would help to mitigate the impact of terrorist attacks from the very beginning. For instance, it could prevent a progressive collapse of a structure and reduce possible impacts of flying fragments. It should be taken into account in urban planning. Public and private entities need to be involved to better take into account protection issues in the design of buildings and other spaces.

2. Assess the necessary **access controls and barriers**, whilst avoiding creating new vulnerabilities. Access controls and barriers should not shift risks and create new targets.

When putting in place security measures, operators should aim to avoid creating new vulnerabilities, such as bottlenecks and long queues that could then become an alternative target. Places of controls and security checks should also be secured against potential threats.[5]

3. Assess the most appropriate **detection technology** for explosives, firearms, bladed arms, as well as chemical, biological, radiological and nuclear agents.

The operators should carefully choose technology fit for their purposes – e.g. scanners with adequate resolution and sensitivity since not all technology is suitable in all areas. This should be based on the vulnerability assessment and in consultation with security experts and manufacturers. Specifications from operators regarding their performance requirements for selecting security equipment should be discussed with manufacturers, including the number of persons that can be screened.

Section 4: Cooperation

1. Appoint **contact points and clarify respective roles and responsibilities** in public-private cooperation on security matters (e.g. between operators, private security and law enforcement authorities) and for a better communication and cooperation on a regular basis.

Public authorities and operators should establish clear communication channels in case of a security event and update each other on the person(s) responsible for particular tasks (e.g. who is in charge of a particular premise, who is responsible for coordination, etc.) so that both sides can clearly and easily know whom to contact. These contacts should be easily reachable and available.

2. Establish **trustful and timely communication and cooperation** that allows for a specific risk and threat information exchange between responsible public authorities, local law enforcement and the private sector.

---

[5] The Commission's Joint Research Centre published guidance on the place of detection at https://www.hindawi.com/journals/ace/2018/3506892/

Public authorities should share risk assessment and information with the operators as appropriate.

3. **Coordinate the work on protection of public spaces** at local, regional and national level and engage in communication and good practice exchanges at all levels including at EU level.

Public authorities should coordinate and support the work on protecting public spaces, which would include clarifying responsibilities for security among the various actors, and engaging in various fora for cooperation.

4. Public authorities, together with operators, should develop and make available **practical recommendations and guidance materials** to detect, mitigate or respond to security threats.

Cooperation between public authorities and the private sector on recommendations and guidance materials is key. Guidance materials, experiences and good practices should be shared extensively.