European Commission

EVALUATION ROADMAP

Roadmaps aim to inform citizens and stakeholders about the Commission's work to allow them to provide feedback and to participate effectively in future consultation activities. Citizens and stakeholders are in particular invited to provide views on the Commission's understanding of the problem and possible solutions and to share any relevant information that they may have.

TITLE OF THE EVALUATION	*Evaluation of the 2008 European Critical Infrastructure Protection Directive*
LEAD DG – RESPONSIBLE UNIT	HOME D2
INDICATIVE PLANNING (PLANNED START DATE AND COMPLETION DATE)	Start first quarter 2018, completion last quarter 2018.
ADDITIONAL INFORMATION	*https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en*

The Roadmap is provided for information purposes only. It does not prejudge the final decision of the Commission on whether this initiative will be pursued or on its final content. All elements of the initiative described by the document, including its timing, are subject to change.

A. Context, purpose and scope of the evaluation

Context

The European Critical Infrastructure Protection Directive (2008/114/EC) of 8 December 2008 establishes a procedure for identifying and designating European Critical Infrastructures (ECI) and a common approach for assessing the need to improve their protection.

It is a key pillar of the European Programme for Critical Infrastructure Protection (EPCIP), which aims at protecting critical infrastructures against all kinds of threats, by an all hazards approach. This means that man-made, technological threats as well as natural disasters should be taken into account in the critical infrastructure protection process, but the threat of terrorism should be given priority.

More specifically, the objectives of the 2008 European Critical Infrastructure Protection Directive are:

- to identify European Critical Infrastructures (ECI), defined as those which disruption or destruction would have a significant impact on at least two Member States;

- to ensure that all identified European Critical Infrastructures are protected, particularly by the creation of an Operator Security Plan (OPS), appropriately and regularly reviewed.

Although the Directive was quickly transposed in the national laws of all Member States, a review conducted by the Commission in 2012, concluded that its application was limited and only a few European Critical Infrastructures (ECIs) were identified and designated. There were also wide discrepancies in the application of the Directive between Member States. Reporting on the application of the Directive was also to some extent irregular. It was also found that the Directive helped to assess the need to improve the protection of ECIs in the transport and energy sectors, but there was no indication that it had actually improved security in these sectors. The conclusions of the review also suggested that the sector-focused approach of the Directive represented a challenge to some Member States, as the analysis of criticalities is not restricted to sectoral boundaries but follows a systems approach, wider and therefore preferable. .

Since then, the pace of identification of European Critical Infrastructures has somewhat accelerated. Currently 89 European Critical Infrastructures are designated. However, the vast majority of these have been designated by two Member States only, and primarily in the energy sector. Other Member States have been more reluctant to identify European Critical Infrastructures. Overall, only a few transport infrastructures have been identified.

In the meantime, the terrorist threat picture for Europe has evolved, with a significant rise in the number of attacks in Europe. Although recent Jihadi terrorism has focused on public spaces rather than infrastructures, critical infrastructure remains an important target for terrorists. Some of the recent attacks targeted transport hubs that can be regarded as both public spaces and critical infrastructure both in the EU (e.g. Brussels airport and metro attack on 22 March 2016) and in neighbouring countries (Istanbul airport attack on 28 June 2016). There has also been at least one serious albeit unsuccessful attempt of attacking an industrial infrastructure by an infiltrated insider, on 26 June 2015 – the target was Air Products gas factory in Saint-Quentin-Fallavier, France. According

to the yearly EU Terrorism Situation and Trend Report (TE-SAT) from 2017, there is also concern over the use of unmanned aerial systems by ISIS, as they could be a vector of attack against critical infrastructures.

There is furthermore a growing concern about hybrid threats, a coordinated combination of hostile activities, where the perpetrator conceals its identity and avoids acts of open warfare. In some recent crises outside the EU (e.g. Ukraine since 2014), hybrid attacks were used with considerable success. The seriousness of this threat was recognized by EU in April 2016 with the adoption of the Joint Communication on countering hybrid threats.

Purpose and scope

The 2012 review of the European Critical Infrastructure Protection Directive already identified a number of issues in its functioning, such as its scope which is limited to energy and transport sectors and the slow pace of identification and designation of ECIs. The present evaluation will further assess the effectiveness, efficiency, relevance, coherence and EU added value of the Directive, thereby analysing to what extent the above-mentioned objectives have been achieved. The evaluation will take into account the outcomes of the 2012 review.

The evaluation will establish the effectiveness and efficiency of the Directive in a context of increased terrorist threat, considering all types of attacks, including insider infiltration, unlawful use of drones and hybrid threats.

It will cover all EU Member States, in the period running from 2008 until today. It will not cover other (non-legislative) elements of the European Programme for Critical Infrastructure Protection (EPCIP).

The evaluation should take into account other efforts of strengthening EU instruments for security, including the adoption of Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (generally known as the NIS Directive).

B. Better regulation

Consultation of citizens and stakeholders

The issue of ensuring resilience of critical infrastructures is important to the whole society, as every single legal and physical person in the EU relies on such infrastructures for many aspects of private and/or professional life. The Commission will therefore carry out consultations in order to receive suggestions for improvements from both operators of critical infrastructures, as well as the users of their services: state and local authorities, commercial enterprises and private citizens. The most relevant feedback is expected from the operators of infrastructures, who deal with security and resilience on a daily basis.

In addition to targeted consultations, a public consultation will be launched in spring 2018, running for a period of minimum 12 weeks. The questionnaire will be available in all 24 official languages of EU and will be accessed via the Commission central public consultation site. The synopsis report (a summary of all consultation results) will be published on the consultation page once these activities are closed. Consultation with MS authorities and operators will take place in autumn 2018 CIP Points of Contact meeting, as it was already the case in 2017.

Data collection and methodology

A first review of Directive 2008/114 was carried out in 2012 and its results were taken into account in a Commission Staff Working Document on a new approach to the EPCIP (SWD(2012) 190 final). Two reports supported the preparation of this review:

- a Study supporting the preparation of the review of the Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures (ECI) and the assessment of the need to improve their protection

- a Study on the potential impacts of options amending Council Directive 2008/114/EC

An external study will be commissioned by the Commission to evaluate the directive, especially taking into account all developments which have occurred since 2012 as well as the new context of increasing threats. A questionnaire addressed to Member States and principal operators of Critical Infrastructures, as well as visits and interviews in Member States will be major elements of this analysis.