EUROPEAN
COMMISSION

Brussels, 23.7.2019
SWD(2019) 310 final

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE EVALUATION

of

COUNCIL DIRECTIVE 2008/114 ON THE IDENTIFICATION AND DESIGNATION OF EUROPEAN CRITICAL INFRASTRUCTURES AND THE ASSESSMENT OF THE NEED TO IMPROVE THEIR PROTECTION

{SWD(2019) 308 final}

Background to the evaluation

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection aims to enhance the protection of critical infrastructure in the European Union. Specifically, the Directive **provides a procedure for the identification and designation of European critical infrastructures (ECIs)** in the energy and transport sectors, as well as **a common approach to the assessment of the need to improve the protection of such infrastructure**. The Directive is **part of the 2006 European Programme for Critical Infrastructure Protection**, which sets out an overall policy approach and framework for critical infrastructure protection (CIP) activities in the EU.

In 2017, the Comprehensive Assessment of EU Security Policy[1] pointed out the need to take a broad view on EU CIP policy. In response, the Commission launched an evaluation aimed at assessing the implementation of the Directive in terms of its **relevance, coherence, effectiveness, efficiency, EU added value and sustainability** in order to provide the Commission with recommendations on how to further strengthen the protection and resilience of critical infrastructure in Europe. **A wide range of stakeholders**, including Member States, operators of critical infrastructure, the public, academia, and EU Institutions and Agencies, were consulted as part of the evaluation.

Main findings

The evaluation found that the technological, economic, social, policy/political and environmental context in which critical infrastructure in Europe operate has changed considerably since the Directive entered into force. In view of these changes and the challenges they pose to CI operations and security, the Directive has partial **relevance**. Furthermore, the Directive is generally **consistent** with relevant European sectoral legislation and policy at international level.

The Directive has been partially **effective** in establishing a common approach to the assessment of the need to improve the protection of ECI due to the generality of some of the Directive's provisions, leaving room for different interpretations by Member States. Certain spill-over effects (e.g. increased CIP awareness about CIP and additional measures at national level) were observed. On **efficiency**, the evaluation found no conclusive evidence that the results attributed to the Directive have been achieved at a reasonable cost. While the costs associated with implementation appear to be limited, it was not possible to assess the Directive's regulatory burden on stakeholders.

The Directive generated **EU added value** insofar as it achieved results (i.e. a common framework for the protection of ECI) that neither national or other European initiatives would otherwise have achieved, or that national or other EU initiatives could have achieved, but only through longer, costlier and less well-defined processes. Certain provisions contained in the Directive were found to have limited added value for many Member States. On

[1] Staff Working Document (2017) 278.

sustainability, several effects generated by the Directive are likely to continue to exist were the Directive to be repealed and not replaced. On the other hand, other effects (e.g. cross-border CIP discussions, reporting requirements) would likely cease.

The evaluation finds that there is **continued support on the part of Member States for EU involvement in CIP policy**, and that there is some concern that the outright repeal of the Directive might have negative effects concerning the protection of ECIs. Member States are keen to ensure that the EU's engagement in the field continues to respect the principle of subsidiarity, supports CIP measures at national level, and facilitates cross-border cooperation, including with third countries outside the Union.

There is clearly room for reflection at EU level on how to further enhance the protection of CI in Europe, including that of the 93 ECIs that have been designated in the energy and transport sectors to date. While some elements of the Directive remain useful, others are of limited value today and could be revisited with the aim of better achieving the Directive's objectives. For instance, there are grounds to consider shifting the focus of EU CIP policy away from asset protection to one that accounts for **interdependencies across a range of different sectors** (much like the NIS Directive does in the field of information and communications technology (ICT)). Furthermore, many national CIP frameworks include measures aimed at strengthening **resilience**. The evaluation also points to the need to review **the current scope of the EU's CIP policy framework** and whether it should encompass additional sectors besides energy and transport.

The external study provides the Commission with a range of recommendations aimed at enhancing the utility of the Directive. Some of these recommendations could be acted on in relatively short order, while others require **more reflection informed by additional consultations with Member States and stakeholders in a wide range of sectors**. Any further action on CIP would need to be coherent with both existing and foreseeable future legislation in order to ensure clear EU added value and to minimise the risk that undue burdens are placed on Member States and CI owners/operators.

Finally, the evaluation shows **an evolution in the nature of the threats facing CI in Europe**. While some threats (like insiders) are evolving, others (like unmanned aerial vehicles or artificial intelligence) are arguably new. While the introduction of improved capabilities (like 5G) will improve efficiencies in various CI sectors, they may also exacerbate existing vulnerabilities or create new ones. In this and other related contexts, the implications of third-country ownership/control of CI in Europe require careful monitoring. For these reasons, **the EU's approach to CIP going forward must be flexible and risk-based** so as to reflect the threats and vulnerabilities that critical infrastructures are likely to face in the decades to come.