Ref. Ares(2020)3202859 - 19/06/2020

European Commission

INCEPTION IMPACT ASSESSMENT

Inception Impact Assessments aim to inform citizens and stakeholders about the Commission's plans in order to allow them to provide feedback on the intended initiative 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 make available any relevant information that they may have, including on possible impacts of the different options.

TITLE OF THE INITIATIVE	Proposal for measures to enhance the protection and resilience of critical infrastructure
LEAD DG (RESPONSIBLE UNIT)	DG HOME, unit D2 Counter-Terrorism
LIKELY TYPE OF INITIATIVE	Legislative proposal
INDICATIVE PLANNING	Q4 2020
ADDITIONAL INFORMATION	https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/protection_en

The Inception Impact Assessment 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 Inception impact assessment, including its timing, are subject to change.

A. Context, Problem definition and Subsidiarity Check

Context

The quality of life of EU citizens and their security, as well as the correct functioning of the internal market, depend on a reliable functioning of critical infrastructures[1] in a wide range of sectors. This requires that adequate efforts are taken to protect key infrastructures from disruptions, be they natural or man-made, unintentional or with malicious intent. Where this fails, these infrastructures must be resilient, i.e. able to 'bounce back' to adequate performance levels within a reasonable amount of time.

In its European Programme for Critical Infrastructure Protection (EPCIP) of 12 December 2006[2], the Commission set out an overall policy approach and framework for critical infrastructure protection (CIP) activities in the EU against all hazards and in all sectors. The four main focus areas of EPCIP are:

- a procedure to identify and designate European critical infrastructures and assess the need to improve their protection (addressed in the European Critical Infrastructure Directive (ECI Directive[3]); limited to the transport and energy sector;
- measures to facilitate the implementation of the EPCIP, including expert groups at EU level, an information-sharing process and a Critical Infrastructure Warning Information Network (CIWIN);
- research on and subsidies for CIP-related measures and projects; and
- a framework for the cooperation with third countries.

In addition, the EU has taken a range of CIP-relevant initiatives[4] in different sectors and on different topics such as energy, transport, civil protection, space, network information systems and foreign direct investment.

---

1 Critical infrastructure means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result to maintain those functions.

2 COM(2006) 786.

3 The European Critical Infrastructure Directive 2008/114/EC (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114) provides a procedure to identify and designate critical infrastructures in the transport and energy sectors that are critical from European perspective (i.e. their disruption would have a significant impact on at least two Member States).

4 A non-exhaustive list of examples of EU instruments introduced in recent years and that are relevant in a CIP context include: Regulation 2017/1938 and Regulation 994/2010 concerning measures to safeguard the security of gas supply; Regulation 1285/2013 on the implementation and exploitation of European satellite navigation systems; Directive 2009/119 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products;

Clearly, the landscape related to critical infrastructure protection has changed in the years since EPCIP was created and the ECI Directive adopted. The recent evaluation of the ECI Directive[5] demonstrated that the current approach is only partially relevant to the context in which these infrastructures operate.

The proposal for additional measures on critical infrastructure protection is included in the Commission work programme 2020 (CWP 2020 - Annex). It will be developed in coordination with other planned/ongoing initiatives in related sectors, notably the review of the Directive on security of network and information systems[6] and the cross-sectoral financial services act on operational and cyber resilience[7].

Problem the initiative aims to tackle

The existing framework for protection and resilience of critical infrastructures is inadequate in the light of increasing interdependencies and evolving risks. As these infrastructures are more reliant upon one another, disruptions in one sector can have immediate and in some cases long-lasting effects on operations in others. As a result, services that are essential for the maintenance of critical societal and/or economic activities can be significantly disrupted. Moreover, some of the disruptions can have severe and cross-border consequences for security, and lead to uncertainty or undermine confidence in the responsible authorities and providers of essential services.

The proposed initiative will therefore aim to address the following aspects that were identified in the recent evaluation of the ECI Directive and subsequent discussions with stakeholders:

- **Discrepancies in the implementation of the ECI Directive and overlapping obligations lead to an uneven playing field for operators:** ECI Directive leaves broad room for interpretation, leading to a wide variance in national approaches and uneven designation of European critical infrastructures. Moreover, since the adoption of EPCIP in 2006 and ECI Directive in 2008, a range of CIP-relevant initiatives in different sectors have been adopted at EU level, and organisations[8] where many EU countries are members have also developed their own frameworks for CIP. There is a possibility to better explore the synergies between these various initiatives. Different obligations (including reporting requirements) for infrastructure operators/owners can create an uneven level playing field in the European single market and additional burden, especially for those operating in different Member States. These differing obligations can also contribute to disparities between the levels of protection of critical infrastructures in the EU.

- **Increased interdependencies and related risk of cascading effects across sectors are not sufficiently taken into account:** While critical infrastructures are more networked, interconnected and reliant upon one another (disruptions in one sector can have cascading effects in other sectors, including cross-border), the EU framework does not provide the mechanism necessary for Member States to identify and manage these interdependencies in a systematic way. Meanwhile, the ECI Directive has a limited sectoral scope, as it focuses solely on the transport and energy sectors, and then only on the designation and protection of a narrow set of European critical infrastructures in these two sectors.

- **Insufficient focus on resilience of critical infrastructure at European level:** A single focus on physical protection does not ensure reliable functioning of critical infrastructures. The attention of Member States and owners/operators of critical infrastructures is on both protection *and* resilience, i.e. that they are capable of quickly 'bouncing back' in the wake of disruptions. This resilience element is only addressed in a horizontal way in the current EU framework as regards cyber risks and threats, making it more difficult for the operators to design suitable business continuity plans and avoid that disruptions adversely affect the operations.

Decision 2019/420 on a Union Civil Protection Mechanism; Regulation 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security; Regulation (EC) 725/2004 enhancing ship and port facility security; or Regulation 1315/2013 on Union guidelines for the development of the trans-European transport network (which has identified a multimodal transport core network covering the most important infrastructure for cross-border transport of persons and goods).

5 SWD(2019) 308 (link).

6 Directive 2016/1148 concerning measures for a high common level of security of networks and information systems across the Union (NIS Directive-link). Commission Work Programme 2020 – Annex I no. 12.

7 Commission Work Programme 2020 – Annex I no. 17.

8 Such as the Organisation for Economic Cooperation and Development (OECD) and the North Atlantic Treaty Organisation (NATO).

- **Risk assessment methodologies vary and coordination and response mechanisms are not sufficiently comprehensive:** The threat picture facing critical infrastructures comprises terrorism, hybrid actions[9], cyber-attacks, insider incidents[10]; potential threats associated with new and emerging technologies (such as drones, 5G, artificial intelligence)[11], or disruption of supply chains. These threats, along with the existing vulnerabilities and the likelihood that they take place, create risk environment that needs to be accounted for. Climate change related challenges[12] and pandemics (as the Corona virus crisis) are also of growing concern. There is a range of different procedures, methodologies and coordination mechanisms in place in Member States and within sectors aimed to assess and address different threats/risks, which in some cases do not necessarily reflect the evolving risks. At the same time, the EU framework does not provide a mechanism to assess and to manage all of these threats/risks in a systematic way. This also makes it difficult for the operators to anticipate the risks, which can in turn impact on their ability to provide essential services in case of disruptions.

The ongoing study that will support the impact assessment process, as well as the input from stakeholders, will help in refining the problem definition.

Basis for EU intervention (legal basis and subsidiarity check)

The choice of the legal basis will be refined depending on the specific measures identified in the impact assessment. The initiative will among other things aim to ensure the provision of essential services through reliable critical infrastructures, in the interest of a well-functioning European economy. It should also help to reduce overlapping obligations for critical infrastructure operators and unnecessary burdens, and ensure a level playing field. For these reasons, Article 114 of the Treaty on the Functioning of the European Union[13] could potentially be used as a legal basis.

The objectives of this initiative can be better achieved at the EU level rather than by EU Member States alone, in view of:

- the cross-border nature of the current and anticipated possible threats and vulnerabilities facing critical infrastructure in the EU;
- the interdependencies that exist between and among critical infrastructures (be they in a single sector or in different ones), and, as a result, the potential for disruptions to have significant cross-border consequences;
- the impact of protective measures on other aspects of common interest, such as safety of infrastructures;
- the fact that some critical infrastructures provide essential services over national borders or even across the entire EU (e.g. space services);
- the fact that only consistent rules can reasonably be expected to reduce the burden on and costs for infrastructure operators acting across the EU, and ensure a level playing field for operators.

In accordance with the principle of proportionality, the proposed measures will not go beyond what is necessary in order to achieve these objectives. The measures will focus on those areas where the EU has the clear potential to provide added value and complement and support the measures already being taken by the Member States.

B. Objectives and Policy options

The overall objective of this initiative is to enhance further the protection and resilience of critical infrastructures in the EU (which in turn will contribute to securing the provision of essential services in the wake of disruptions), taking into account the increasingly deep nature of sectoral interdependencies and the evolving risks. The NIS Directive already demonstrated that there was a need to ensure the

[9] The hybrid threats refer to the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare.

[10] Insider threats are posed by current or former employees who can misuse their access rights within an organisation, to harm and cause damage.

[11] Such as disruptions to critical infrastructure operations (including aviation) due to unauthorised drone incursions.

[12] Such as lack of water for cooling stations at nuclear power plants due to more frequent drought events.

[13] Official Journal C 326 , 26/10/2012 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT)

security of network and information systems used by operators for the provision of services that are essential for the maintenance of critical societal or economic activities against cyber threats. These operators of essential services should also be secure and resilient against a range of non-cyber risks.

More specifically, the initiative aims to:

- Ensure greater coherence as to the EU's overall critical infrastructure protection approach;
- Ensure a level playing field for operators across the EU by providing them with consistent requirements, including reporting mechanisms;
- Ensure that all relevant sectors providing essential services are included in the critical infrastructure protection approach, and that cross-sectoral/cross-border disruptions are effectively managed;
- Put in place new/refine existing mechanisms aimed at enhancing further the ability of Member States to protect and ensure the resilience of national critical infrastructures;
- Ensure a higher level of understanding of the risks/threats that critical infrastructures face now and might come to face in the future, as well as the means to address them;
- Improve information exchange and cooperation.

In achieving these objectives, it will be necessary to acknowledge and take into account the existing regulatory requirements, initiatives and cooperation/information-sharing mechanisms established within the framework of other relevant sectoral and cross-sectoral initiatives already providing some elements of critical infrastructure protection (such as in aviation and maritime transport[14]).

At this preliminary stage of reflection, the Commission is considering several policy options to achieve the pursued objectives. The ongoing study that will support the impact assessment process, and input from stakeholders will help identify policy options and relevant measures. Options to be considered include:

Option 1 – Baseline scenario under which the current EU framework would remain in place without changes. Under the ECI Directive, the number of designated European Critical Infrastructures would be unlikely to increase significantly over the current state of play (as of March 2020: 94 in total, of which 88 in the energy sector and 6 in the transport sector. In 2019: +1) Furthermore, the interpretation of existing ECI provisions would continue to allow Member States to pursue heterogonous approaches to infrastructure identification and designation. This would have limited impact on improving the protection of critical infrastructures.

Option 2 – Non-legislative measures at EU level

Under this option, the EPCIP programme would be improved by non-legislative measures such as awareness-raising, education and training, exchange of information and best practices (also through a technological environment, cooperation groups, peer reviews, a knowledge hub) or organisation of stress tests and exercises which are facilitated or (co-)financed by the EU in order to better address the cross-border nature of the current and anticipated possible threats and vulnerabilities facing critical infrastructure in the EU.

Option 3 – New requirements for European critical infrastructures

Under this option, the current European Critical Infrastructure Directive would be revised following the recommendations that were generated during its recent evaluation. This could for instance include a clarification of existing requirements/definitions to further align implementation in Member States (thus contributing to more consistent requirements for the operators); an update of existing provisions to take into account recent sectoral legislation; or revised methodology to identify European critical infrastructures (better taking into account increased interdependencies and evolving risks). The approach would remain asset focused (i.e. focused on the designation of critical infrastructures at EU level), with the scope potentially expanded to include sectors beyond energy and transport.

[14] Regulation (EC) No. 300/2008; Regulation (EU) 2015/1998; Regulation (EC) 725/2004; Directive 2005/65/EC; Regulation (EC) 324/2008.

Option 4 – New requirements focused on essential services

Under this option, the Commission would propose a general framework defining the main principles and expected outcomes of a EU critical infrastructure protection policy, leaving it to sectoral or specific cross-sectoral legislation to determine more detailed requirements where necessary. Such a general framework could for instance include: baseline requirements for protection and resilience (thus providing a more coherent approach and consistent obligations for operators) and their monitoring by Member States; means to assess cross-sectoral and cross-border interdependencies and related threats; or an early warning and information mechanism at EU level (in order to better address the evolving risks/threats facing critical infrastructures); or criteria for the vetting of staff with access to critical infrastructure. In terms of the approach, the focus would shift away from identifying and protecting a narrow set of European critical infrastructures to the protection and resilience of infrastructures providing essential services (thereby ensuring that all relevant sectors providing essential services are included in the European critical infrastructure protection policy, and aligning it with the policy reflected in the NIS Directive).

C. Preliminary Assessment of Expected Impacts

Likely economic impacts

A preliminary list of likely economic impacts may include:

- reduction of network disruptions and of related negative impacts on businesses' operations
- market efficiencies from optimised rules/requirements
- increased level-playing field among operators of critical infrastructures across the EU
- costs of the management of critical infrastructures possibly impacting prices for essential services (indirect impacts)

Likely social impacts

A preliminary list of likely social impacts may include:

- better protection against threats that critical infrastructures face and swifter recovery (bouncing-back) of essential services after an incident because of more resilient critical infrastructures
- increased security for citizens
- impact on public health and higher safety for users (incl. infrastructure operators) due to better protected infrastructures
- increased awareness about security
- strengthened social cohesion and solidarity amongst Member States
- reduced disparities between the levels of development of the various regions because of more reliable provision of services

Likely environmental impacts

Environmental impacts may also be of relevance for this initiative – better protected and more resilient infrastructures can lead to fewer incidents, and thus prevent adverse effects on environment.

Likely impacts on fundamental rights

A preliminary list of likely impacts on fundamental rights may include impacts for the right to property and for the right to conduct a business, the freedom to choose an occupation and right to engage in work and the freedom of movement.

Likely impacts on simplification and/or administrative burden

The impact assessment will assess the effects of each option in relation to the anticipated compliance costs (these could be linked to enhanced requirements on operators to take certain protective measures; or more thorough risk assessment obligations on Member States) and/or administrative burden (these could be linked to information-sharing obligations on operators and reporting obligations on Member States).

The streamlining of the responsibilities and procedures related to critical infrastructure protection and resilience could be expected to result in a decreased administrative burden on the part of both operators and competent authorities in the Member States.

D. Evidence Base, Data collection and Better Regulation Instruments

Impact assessment

An impact assessment is currently being prepared to both support the preparation of this initiative and

to inform the Commission's decision. The impact assessment will be carried out during Q2-Q3 of 2020.

Evidence base and data collection

Building on the ECI Directive evaluation, the Commission will collect more evidence through several different sources:

- A study that will inform the impact assessment process is ongoing. It will use a combination of qualitative and quantitative methodologies in order to collect relevant data and contextual information necessary for the analysis. The study will account for the entire scope of the EPCIP, including the ECI Directive, as well as other CIP-relevant initiatives taken at European level on both a sectoral and cross-sectoral basis.
- The Commission will also draw on existing studies, reviews and evaluations concerning European CIP policy, including the EPCIP, the ECI Directive specifically[15], and other relevant EU measures.
- The input collected through various consultation activities outlined below.

Consultation of citizens and stakeholders

The proposal will be based on a number of targeted consultations with a wide range of stakeholders, including competent Member States authorities, operators of critical infrastructures and other industry stakeholders, international organisations, as well as academia and think-tank representatives. The consultation activities will involve interviews, surveys and workshops. The following consultation activities are planned:

- Web-based survey with relevant authorities in Member States (completed), followed by in-depth interviews with representatives of 10 Member States.
- Interviews with relevant international organisations; representatives of EU institutions and representatives of academia and think tanks.
- Consultative workshops with Member States, critical infrastructure operators and national and European associations of operators in different sectors – focused on validation of problem definition / baseline scenario; and on definition of possible policy measures[16].
- Written consultation of Member States, critical infrastructure operators and experts (through the European Reference Network for Critical Infrastructure Protection (ERNCIP) network), at a more advanced stage of impact assessment work, with focus on policy measures and their impact.

The results of the public consultation carried out in 2019 as part of the evaluation of the ECI Directive will also be used.

The consultation of Member States will be accomplished through the relevant Council Working Groups and an existing formal expert group (the Critical Infrastructure Protection Points-of-Contact). In order to raise stakeholder awareness about the various ways that they may be involved in the consultations, the Points-of-Contact group was requested to forward relevant information within their respective networks as appropriate.

In addition to the feedback received on the Inception Impact Assessment, no public consultation is planned for this initiative, which will benefit from a range of targeted consultations and from the results of the public consultation carried out during the evaluation stage.

Will an Implementation plan be established?

If a legislative approach is taken to enact this initiative and if the new rules take the form of a directive, an implementation plan will be established.

[15] SWD(2019) 308 (link).

[16] Some of the workshops will be replaced by focused written surveys to limit the burden (as many of the targeted stakeholders are currently in the front line of responding to the Covid-19 crisis, affecting their availability for any other activities).