



EU COUNCIL ~FACTSHEET~

EUROPEAN CRITICAL INFRASTRUCTURE

**Justice and Home Affairs Council
Luxembourg, 5 June 2008**

The Council reached political agreement on a directive on the identification and designation of European Critical Infrastructure (ECI) and the assessment of the need to improve their protection [\(9403/08\)](#).

The directive establishes the necessary procedure for the identification and designation of ECI and a common approach to the assessment of the needs to improve the protection of such infrastructure in order to contribute to the protection of people. The directive concentrates on the energy and transport sector and will be reviewed after three years, in order to assess its impact and the need to include other sectors within its scope, such as the Information and Communication Technology (ICT) sector.

Background

Following the Madrid terrorist attack (March 2004), the European Council asked the Council to prepare an overall strategy to enhance the protection of critical infrastructure in the European Union.

The Commission adopted on October 2004 a Communication on Critical Infrastructure Protection in the Fight against Terrorism which put forward suggestions on what would enhance European prevention, preparedness and response to terrorist attacks involving Critical Infrastructures [\(13979/04\)](#).

P R E S S

In December 2006, the Commission presented a Communication on a European Programme for Critical Infrastructure Protection (EPCIP) which sets out the principles, processes and instruments proposed to implement EPCIP (16932/06). The Commission also presented its proposal for a directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection (16933/06).

What is an "European Critical Infrastructure"?

"European Critical Infrastructure", are those assets, systems or parts thereof located in EU member states which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people (e.g. electricity, gas and oil production, transport and distribution ; telecommunication ; agriculture ; financial and security services ; etc.), and the disruption or destruction of which would have a significant impact on at least two EU member states.

Critical infrastructure industries are becoming more and more interdependent as the economic, technological, and social processes of globalization intensify. Therefore, the damage or loss of a piece of infrastructure in one member state may have negative effects on several others and on the European economy as a whole. Because of this trans-boundary dimension, an integrated EU-wide approach would complement and have an added value to the already existing national programmes for critical infrastructure protection in place in the member states.

Identification and designation of European Critical Infrastructure

The **identification** process has four main steps:

- Step 1:** Each member state shall apply sectoral criteria according to the characteristics of individual energy and transport infrastructure in order to make a first selection of "*potential critical infrastructure*";
- Step 2:** Checking if the infrastructure it matches the criteria established in the critical infrastructure
- Step 3:** Establishment of trans-boundary effect of the infrastructure (i.e. affecting two or more member states);
- Step 4:** Application of the following cross-cutting criteria to the infrastructure::
- casualties criterion (assessed in terms of potential number of fatalities or injuries);
 - economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects);
 - public effects criterion (assessed in terms of the impact of public confidence, public health and disruption of daily life; including the loss of essential services).

Infrastructure that satisfy all the above criteria, will be **designated** as "European Critical Infrastructure".

Protection of European Critical Infrastructure

Each designated European Critical Infrastructure shall have an **Operator Security Plan (OSP)** covering *inter alia* an identification of important assets, a risk analysis based on major threat scenarios and vulnerability of each asset, identification, selection and prioritisation of counter-measures and procedures.

A **Security Liaison officer** will function as the point of contact for security issues between European Critical Infrastructure owner/operator and the relevant member state authority.

Every two years, each member state shall forward to the Commission information on threats and risks encountered per European Critical Infrastructure sector. On the basis of those reports, the Commission and the member states shall examine whether further protection measures at the EU level should be considered.
