Identification and designation of European critical infrastructures and assessment of the need to improve their protection

2006/0276(CNS) - 12/12/2006 - Legislative proposal

PURPOSE: to create a horizontal framework for the identification and designation of European Critical Infrastructures and for the assessment of needs to improve their protection.

PROPOSED ACT: Council Directive.

BACKGROUND: the security and economy of the European Union as well as the well-being of its citizens depends on certain infrastructure and the services they provide. The destruction or disruption of infrastructure providing key services could entail the loss of lives, the loss of property, a collapse of public confidence and moral in the EU. Any such disruptions or manipulations of critical infrastructure (energy, communication, water, food provisioning, health, transport, etc) should, to the extent possible, be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the Member States, their citizens and the European Union.

In order to counteract these potential vulnerabilities the European Council requested in 2004 the development of a European Programme for Critical Infrastructure Protection. Since then, a comprehensive preparatory work has been undertaken, which has included the organisation of relevant seminars, the publication of a Green Paper and discussions with both public and private stakeholders.

With this in mind, an EPCIP Communication has been developed establishing a horizontal framework concerning the protection of critical infrastructures in Europe.

CONTENT: as part of the EPCIP framework dealing specifically with European Critical Infrastructures, it is necessary to include a proposal for a Directive of the Council on the **identification and designation of European Critical Infrastructure** and the assessment of the need to improve their protection. The proposed Directive establishes the necessary procedure for the identification and designation of European Critical Infrastructure (ECI), and a **common approach** to the assessment of the needs to improve the protection of such infrastructure.

The ECI Directive lays down the procedure on how to identify and designate ECI:

- The Commission together with the Member States and relevant stakeholders develop cross-cutting and sectoral criteria for the identification of ECI, which are then adopted through the comitology procedure.

- The cross-cutting criteria are developed on the basis of the severity of the disruption or destruction of the CI. The severity of the consequences of the disruption or destruction of a particular infrastructure should be assessed on the basis, where possible, of: public effect (number of population affected); economic effect (significance of economic loss and/or degradation of products or services); environmental effect; political effects; psychological effects.

- Each Member State then identifies those infrastructures which satisfy the criteria.

- Each Member State then notifies the Commission of the critical infrastructures which satisfy the established criteria.

- Following the identification procedure the Commission prepares a **draft list of ECI**. The draft list is based on the notifications received from the Member States and other relevant information from the Commission. The list is then adopted through comitology.

Furthermore, the proposed Directive only imposes two obligations on the owners/operators of those critical infrastructures, which are designated as European Critical Infrastructures. These include:

1. The establishment of an **Operator Security Plan** which would identify the ECI owners' and operators' assets and establish relevant security solutions for their protection. Annex 2 of the ECI Directive provides the minimum contents of such OSPs including:

- identification of important assets;

- a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact shall be conducted;

identification, selection and prioritisation of counter-measures and procedures with a distinction between:

- **Permanent security measures**, which identify indispensable security investments and means which cannot be installed by the owner/operator at short notice. This heading will include information concerning general measures; technical measures (including installation of detection, access control, protection and prevention means); organizational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems.

- **Graduated security measures**, which are activated according to varying risk and threat levels. Once an OSP has been created, each ECI owner/operator should submit it to the relevant Member State authority. Each Member State will setup a supervisory system concerning OSPs which will ensure that sufficient feedback is given to the ECI owner/operator concerning the quality of the OSP and in particular the adequacy of the risk and threat assessment.

2. The designation of a **Security Liaison Officer** (SLO). Article 6 of the ECI Directive requires all CI owners/operators designated as ECI to appoint an SLO. The SLO would function as the point of contact for security issues between the ECI and the relevant CIP authorities in the Member States. The SLO would therefore receive all relevant CIP related information from the Member State authorities and would be responsible for providing relevant information from the ECI to the Member State.

Lastly, the Commission shall take **appropriate measures to protect information** subject to the requirement of confidentiality to which it has access or which is communicated to it by Member States.

For more details concerning the financial implications of this measure, please refer to the financial statement.