Fight against terrorism: Critical Infrastructure Warning Information Network (CIWIN)

2008/0200(COD) - 27/10/2008 - Legislative proposal

PURPOSE: to establish a critical infrastructure warning information network (**CIWIN**) to strengthen information-sharing on critical infrastructure protection between EU Member States.

PROPOSED ACT: Council Decision.

BACKGROUND: the security and economy of the European Union as well as the well-being of its citizens depend on certain infrastructure and the services they provide: telecommunication and energy networks, financial services and transport systems, health services, and the provision of safe drinking water and food, etc. Any destruction or disruption of infrastructure providing key services, on one hand, and an inappropriate response to this kind of event, on the other, could entail loss of life, loss of property and a collapse of public confidence in the EU. Critical infrastructure in the European Union is currently subjected to a varying puzzle of protective measures and obligations, with no minimum standards being applied horizontally.

In June 2004, the European Council asked the Commission to prepare an overall strategy to protect critical infrastructure which lead to the proposed creation of a European Programme for Critical Infrastructure Protection (EPCIP) (see COM(2006)0786). It also adopted conclusions calling on the Commission to set up a Critical Infrastructure Warning Information Network (CIWIN). In December 2006, the Commission proposed a Directive on the identification and designation of European Critical Infrastructure (ECI) (see CNS/2006/0276). Together, these documents set out the framework for infrastructure protection in the EU. The CIWIN initiative is part of EPCIP, being concerned more specifically with the information-sharing process between EU Member States and an information technology system to support that process.

CONTENT: the aim of the proposed Decision is to set up a **secure information, communication and alert system** – Critical Infrastructure Warning Information Network (**CIWIN**) - with the aim of assisting Member States to exchange information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risks related critical infrastructure protection. Critical Infrastructure shall mean those assets, systems or parts thereof located in Member States which are 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 of the failure to maintain those functions.

Participation: participation in and use of CIWIN is open to all Member States. The participation to CIWIN shall be conditional upon the signature of a Memorandum of understanding that contains technical and security requirements applicable to CIWIN, and information on the sites to be connected to CIWIN.

Functionalities: the CIWIN shall consist of two main functions:

1) an **electronic forum** for the CIP related to information exchange which shall be composed of **fixed areas** and **dynamic areas**. Fixed areas shall be included in the system on a permanent basis. While their content may be adjusted, the areas may not be removed, renamed or new areas added (Annex I contains a list of fixed areas such as Member State areas, sector areas (chemical industry; energy; financial; food; health; ICT; nuclear fuel-cycle industry; space, transport; and water, etc), CIWIN executive areas,). Dynamic areas shall be created upon demand, and shall serve a specific purpose. Their existence shall be terminated upon fulfilment of their initial purpose (Annex II

contains a list of dynamic areas to be created upon the establishment of the CIWIN such as expert working group area, alert areas and special topics area). to focus on specific topics;

2) a **rapid alert functionality** that shall enable participating Member States and the Commission to post alerts on immediate risks and threats to critical infrastructure.

Respective roles of the Member States and the Commission in the CIWIN:

- participating **Member States** shall designate a CIWIN Executive and notify the Commission thereof. CIWIN Executive shall be responsible for granting or denying access rights to the CIWIN within the relevant Member State. Participating Member States shall provide access to the CIWIN in compliance with the guidelines adopted by the Commission and shall
- provide and regularly update relevant CIP information of common EU interest;the **Commission** shall be responsible for the technical development and management of the CIWIN, including the IT structure thereof and the elements for information exchange; laying down guidelines on the terms of use of the system, including confidentiality, transmission, storage, filing and deletion of information. It shall also establish the terms and procedures for granting full or selective access to the CIWIN. It shall appoint the CIWIN Executive, responsible for granting or denying access rights to the CIWIN within the Commission and shall provide and regularly update relevant CIP information of common EU interest.

Level of security: the CIWIN shall be established as a secure classified system, and shall be capable of handling information up to the level of RESTREINT UE. The Commission shall decide on the most appropriate technological platform for CIWIN and users shall meet the technical requirements established by the Commission. The security classification of the CIWIN shall be upgraded as appropriate. Users' rights to access documents shall be on a “need to know” basis and must at all times respect the author’s specific instructions on the protection and distribution of a document.

Member States and the Commission shall take the necessary security measures:

- to prevent any unauthorised person from having access to the CIWIN;
- to guarantee that, when using the CIWIN, authorised persons have access only to data which are within their sphere of competence;
- to prevent information on the system from being read, copied, modified or erased by unauthorised persons.

Budgetary implication: the costs incurred in connection with the operation, maintenance and central functioning of the CIWIN shall be borne by the Community budget (see the accompanying financial statement). Costs related to users' access to CIWIN within participating Member States shall be borne by participating Member States.

This Decision shall apply as from 1 January 2009. The Commission shall review and evaluate the operation of the CIWIN every 3 years, and shall submit regular reports to the Member States.