Basic information

2008/0200(COD) COD - Ordinary legislative procedure (ex-codecision procedure) Decision	Procedure lapsed or withdrawn
Fight against terrorism: Critical Infrastructure Warning Information Network (CIWIN) **Subject** 7.30.20 Action to combat terrorism	

Key players

Council of the European Union	
European Commission	Commission DG: Justice and Consumers Commissioner: REDING Viviane

Key events

Date	Event	Reference	Summary
27/10/2008	Legislative proposal published	COM(2008)0676	Summary
20/11/2008	Committee referral announced in Parliament, 1st reading		
31/03/2009	Vote in committee, 1st reading		Summary
03/04/2009	Committee report tabled for plenary, 1st reading	A6-0228/2009	
22/04/2009	Decision by Parliament, 1st reading	T6-0227/2009	Summary
22/04/2009	Results of vote in Parliament		
01/12/2009	Formal reconsultation of Parliament		
02/12/2009	Additional information		Summary
02/06/2012	Proposal withdrawn by Commission		Summary

Technical information

Procedure reference	2008/0200(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Decision
Legal basis	Treaty on the Functioning of the European Union TFEU 196-p2
Stage reached in procedure	Procedure lapsed or withdrawn
Committee dossier	LIBE/7/02348

	LIBE/6/69256

Documentation gateway				
European Parliament				
Document type	**Committee**	**Reference**	**Date**	**Summary**
Committee draft report		PE419.940	18/02/2009	
Specific opinion	JURI	PE423.705	01/04/2009	
Committee report tabled for plenary, 1st reading/single reading		A6-0228/2009	03/04/2009	
Text adopted by Parliament, 1st reading/single reading		T6-0227/2009	22/04/2009	Summary

European Commission

Document type	Reference	Date	Summary
Legislative proposal	COM(2008)0676	27/10/2008	Summary
Document attached to the procedure	SEC(2008)2701	27/10/2008	
Document attached to the procedure	SEC(2008)2702	27/10/2008	
Commission response to text adopted in plenary	SP(2009)3507	25/06/2009	

Additional information		
Source	**Document**	**Date**
National parliaments	IPEX	
European Commission	EUR-Lex	

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.

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

2008/0200(COD) - 22/04/2009 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 599 votes to 38, with 35 abstentions, a legislative resolution amending, under the consultation procedure, the proposal for a Council decision on a Critical Infrastructure Warning Information Network (CIWIN).

The main amendments were as follows:

Rapid Alert System: the text is amended so that references to an alert system are deleted. Parliament felt that further analysis and evaluation is needed. The text states that the first evaluation of CIWIN should also include an in-depth analysis of the necessity of adding a new functionality to CIWIN, namely the technical facility of a rapid alert system (RAS). This functionality should enable Member States and the Commission to post alerts on immediate risks and threats to critical infrastructure, taking into account all the necessary security requirements.

Participation: the text is amended in order to render the participation of Member States obligatory. Parliament deletes references to "Participating Member State" and “Participation”.

Functionality and structure: the resolution adds that the technical platform for CIWIN shall be present in at least one secure location in each Member State .

Annex I contains a list of fixed areas, but this does not preclude the inclusion of new areas if the functioning of the system demonstrates that this is necessary.

Role of the Commission: the Commission shall monitor the functioning of the CIWIN system.

Security: a new clause states that in Member States, the exchange of sensitive information uploaded onto CIWIN between authorised users and third parties shall be subject to the prior authorisation of the owner of that information and shall take place in accordance with relevant Community and national law.

Requirements relating to information included in CIWIN: a new article states that for any information or documents uploaded in the system an automatic translation will be possible. The Commission shall, in collaboration with CIP contact points, develop a list of key words for each sector which could be used when uploading or searching for information in CIWIN.

User Guidelines: these will be established in accordance with the advisory procedure.

Report: the Commission, using **specially developed indicators** for monitoring progress, shall review and evaluate the operation of the CIWIN every 3 years. It will report, inter alia, to the European Parliament, the Committee of Regions and the European Economic and Social Committee, and will, in particular, assess the participation of each Member State in the CIWIN system as well as the possibility of upgrading CIWIN to include a RAS functionality.

Lastly, the **date of effect** should be the date of publication in the OJ rather than 1 January 2009.