COUNCIL OF
THE EUROPEAN UNION

Brussels, 11 May 2007

9504/07

LIMITE

PROCIV 74
JAI 237
COTER 42
ENER 135
TRANS 158
TELECOM 64
ATO 71
ECOFIN 203
ENV 259
SAN 94
CHIMIE 13
RECH 135
DENLEG 34
RELEX 340

Interinstitutional File:
2006/0276 (CNS)

OUTCOME OF PROCEEDINGS

from:	Working Party on Civil Protection
on:	23 April 2007
No. Cion prop. :	16933/06 PROCIV 273 JAI 725 COTER 64 ENER 323 TRANS 345 TELECOM 133 ATO 174 ECOFIN 472 ENV 713 SAN 270 CHIMIE 43 RECH 365 DENLEG 61 RELEX 929 + ADD 1 + ADD 2
Subject:	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

At its meetings on 13 February and 23 April 2007 the Working Party on Civil Protection examined, with the participation of critical infrastructure protection experts, the visas and articles 1 and 2 of the above-mentioned Commission proposal. Delegations will find in the Annex the text as it stands following the proceedings of the Working Party.

DRAFT [1]

DIRECTIVE OF THE COUNCIL

on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection[2]

(Text with EEA relevance)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 308 thereof,

[Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 203 thereof,][3]

Having regard to the proposal from the Commission[4],

Having regard to the opinion of the European Parliament[5],

Having regard to the opinion of the European Central Bank[6],

Whereas[7]:

(1) In June 2004, the European Council asked for the preparation of an overall strategy to protect critical infrastructures[8]. In response, on 20 October 2004, the Commission adopted a Communication on Critical Infrastructure Protection in the Fight against Terrorism[9] which put forward suggestions as to what would enhance European prevention of, preparedness for and response to terrorist attacks involving critical infrastructures.

---

1 **Bolds and strikeouts mark the modifications in the Commission proposal**
2 **General scrutiny reservation by <u>all delegations.</u>**
3 **Scrutiny reservation by <u>DE</u> regarding the use of Article 203 of the *Treaty establishing the European Atomic Energy Community* as a legal basis.**
4 OJ C […], […], p. […].
5 OJ C […], […], p. […].
6 OJ C […], […], p. […].
7 **The recitals will be examined following agreement on the articles.**
8 10679/2/04 REV 2.
9 13979/04

(2) On 17 November 2005 the Commission adopted a Green Paper on a European Programme for Critical Infrastructure Protection[10] which provided policy options on the establishment of the programme and the Critical Infrastructure Warning Information Network (CIWIN). The responses received to the Green Paper clearly showed the need to set up a Community framework concerning critical infrastructure protection. The need to increase the critical infrastructure protection capability in Europe and to help reduce vulnerabilities concerning critical infrastructures was acknowledged. The importance of the principle of subsidiarity and of stakeholder dialogue was emphasised.

(3) In December 2005 the Justice and Home Affairs Council called upon the Commission to make a proposal for a European Programme for Critical Infrastructure Protection (EPCIP) and decided that it should be based on an all-hazards approach while countering threats from terrorism as a priority. Under this approach, manmade, technological threats and natural disasters should be taken into account in the critical infrastructure protection process, but the threat of terrorism should be given priority. If the level of protection measures against a particular high level threat is found to be adequate in a critical infrastructure sector, stakeholders should concentrate on other threats to which they are still vulnerable.

(4) The primary responsibility for protecting critical infrastructures currently falls on the Member States and the owners/operators of critical infrastructures. This should not change.

(5) There are a certain number of critical infrastructures in the Community, the disruption or destruction of which would affect two or more Member States or a Member State other than that in which the critical infrastructure is located. This may include transboundary cross-sector effects resulting from interdependencies between interconnected infrastructure. Such European critical infrastructures should be identified and designated by means of a common procedure. The need to improve the protection of such critical infrastructures should be assessed under a common framework. Bilateral schemes for cooperation between Member States in the field of critical infrastructure protection constitute a well established and efficient means of dealing with transboundary critical infrastructure. EPCIP should build on such cooperation.

(6) Since various sectors have particular experience, expertise and requirements concerning critical infrastructure protection, a Community approach to critical infrastructure protection should be developed and implemented taking into account sector specificities and existing sector based measures including those already existing at EU, national or regional level, and where relevant cross-border mutual aid agreements between owners/operators of critical infrastructure already in place. Given the very significant private sector involvement in overseeing and managing risks, business continuity planning and post-disaster recovery, a Community approach will need to encourage full private sector involvement. The establishment of a common list

[10] 14910/05

of critical infrastructure sectors is necessary in order to facilitate the implementation of the sector-by-sector approach to critical infrastructure protection.

(7) Each owner/operator of European critical infrastructure should establish an Operator Security Plan identifying critical assets and laying down relevant security solutions for their protection. The Operator Security Plan should take into account vulnerability, threat and risk assessments, as well as other relevant information provided by Member State authorities.

(8) Each owner/operator of European critical infrastructure should designate a Security Liaison Officer in order to facilitate cooperation and communication with relevant national critical infrastructure protection authorities.

(9) The efficient identification of risks, threats and vulnerabilities in the particular sectors requires communication both between owners/operators of European critical infrastructure and the Member States, and between the Member States and the Commission. Each Member State should collect information concerning European critical infrastructures located within its territory. The Commission should receive generic information from the Member States concerning vulnerabilities, threats and risks, including where relevant information on possible gaps and cross-sector dependencies, which should be the basis for the development of specific proposals on improving the protection of ECI, where necessary.

(10) In order to facilitate improvements in the protection of European critical infrastructures, common methodologies should be developed for the identification and classification of vulnerabilities, threats and risks to infrastructure assets.

(11) Only a common framework can provide the necessary basis for a coherent implementation of measures to protect European critical infrastructure and clearly define the respective responsibilities of all relevant stakeholders. Owners/operators of European critical infrastructure should be given access to best practices and methodologies concerning critical infrastructure protection.

(12) Effective protection of critical infrastructure requires communication, coordination, and cooperation at national and Community level. This is best achieved through the nomination of CIP Contact Points in each Member State, who should coordinate CIP issues internally, as well as with other Member States and the Commission.

(13) In order to develop Critical Infrastructure Protection activities in areas which require a degree of confidentiality, it is appropriate to ensure a coherent and secure information exchange in the framework of this Directive. Certain Critical Infrastructure Protection information is of such nature that its disclosure would undermine the protection of the public interest as regards public security. Specific facts about a critical infrastructure asset, which could be used to plan and act with a view to causing unacceptable consequences for critical infrastructure installations should be classified and access granted only on a need-to-know basis, both at Community level and at Member State level.

(14) Information sharing regarding Critical Infrastructure should take place in an environment of trust and security. The sharing of information requires a relationship of trust such that companies and organisations know that their sensitive data will be sufficiently protected. To encourage information sharing, it should be clear for the industry that the benefits of providing Critical Infrastructure related information outweigh the costs for the industry and society in general. Critical Infrastructure Protection information exchange should therefore be encouraged.

(15) This Directive complements existing sectoral measures at Community level and in the Member States. Where Community mechanisms are already in place, they should continue to be used and will contribute to the overall implementation of this Directive.

(16) The measures necessary for the implementation of this Directive should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission[11].

(17) Since the objectives of this Directive, namely the creation of a procedure for the identification and designation of European Critical Infrastructures, and a common approach to the assessment of the needs to improve the protection of such infrastructures, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale of the action, be better achieved at Community level, the Community may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(18) This Directive respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union.

HAS ADOPTED THIS DIRECTIVE:

Article 1
Subject-matter

This directive establishes a procedure for the identification and designation of European Critical Infrastructures, and a common approach to the assessment of the needs to improve the protection of such infrastructures **in order to contribute to the protection of people**. **Such an approach shall be based on an all-hazard approach, while recognizing the threat from terrorism as a priority.**[12]

---

11 OJ L 184, 17.7.1999, p. 23.

12 **New wording proposed by Pres in order to take into account that, following the *"Council conclusions on principles for EPCIP"* (14689/05, para. 5), some delegations highlighted that the protection of critical infrastructures should be based on an all-hazard approach, whereas others stressed that these conclusions recognized the threat from terrorism as a priority.**
Scrutiny reservation by SE.
GR suggested to mention first the "*threat from terrorism*" and only afterwards the "*all-hazard approach*".

Article 2
Definitions

For the purpose of this directive:

a) "Critical Infrastructure" means those assets[13] or parts thereof which are essential for the maintenance of [critical][14] societal functions, [including the supply chain][15], health, safety, security, economic or social well-being of people;

b) "European Critical Infrastructure" means critical infrastructures the disruption or destruction of which would [significantly affect][16] [two][17] or more Member States, [or a single Member State if the critical infrastructure is located in another Member State][18]. This includes effects resulting from cross-sector dependencies on other types of infrastructure;

[c) "severity" means the impact of the disruption or destruction of a particular infrastructure, with reference to:

- public effect (number of members of the population affected);
- economic effect (significance of economic loss and/or degradation of products or services);
- environmental effect;
- political effects;
- psychological effects[19]
- public health consequences;[20]][21]

AT opposed to the inclusion of the second sentence ("*Such an …").

13 **ES/FR/IT/NL/SE/UK suggested inserting "*and systems*"; IT/UK/Cion suggested mentioning also "*services*" explicitly.**

14 **In order not to repeat the word "*critical*" in the text of the definition ES suggests replacing it by "*fundamental*" or "*important*". Pres considers to suggest "necessary for the maintenance of essential societal functions"; scrutiny reservation by NL.**

15 **Deletion of "*supply chain*" requested by AT as in the past no agreement on this notion could be found in the Working Group on Transport (Horizontal questions)**

16 **FR suggested "*have a serious impact on*"**

17 **"Three" suggested by EE/DK/NL/UK; SE supported this view but questioned, in the first place, whether there was a need for a legally binding instrument at all.**

18 **Depending on the outcome of the discussions on the first part of this sentence ("*two*" or "*three*") this part of the sentence may be changed as well.**

19 **Clarification requested by DE/UK**

20 **IT/NL requested the inclusion of two additional elements in the definition : duration of the disruption and possible alternatives to the relevant infrastructure**

21 **DE/FI/SE/UK suggested that the term "*severity*" be defined only in Article 3 para. 1; Pres suggested to discuss article 2 para. c) together with article 3**

d) ["vulnerability" means a characteristic of an element of the critical infrastructure's design, implementation, or operation that renders it susceptible to disruption or destruction by a threat and includes dependencies on other types of infrastructure;][22]

e) ["threat" means any indication, circumstance, or event with the potential to disrupt or destroy critical infrastructure, or any element thereof;]

f) ["risk" means the possibility of loss, damage or injury having regard to the value placed on the asset by its owner/operator and the [impact of loss or change][23] to the asset, and the likelihood that a specific vulnerability [will be exploited][24] by a particular threat;]

g) ["Critical[25] Infrastructure Protection Information" means specific facts about a critical infrastructure asset, which if disclosed could be used to plan and act with a view to guaranteeing failure or causing unacceptable consequences for critical infrastructure installations.[26]]

Article 3
Identification of European Critical Infrastructure

1. The cross-cutting and sectoral criteria to be used to identify European Critical Infrastructures shall be adopted in accordance with the procedure referred to in Article 11(3). They may be amended in accordance with the procedure referred to in Article 11(3).

   The cross-cutting criteria having a horizontal application to all critical infrastructure sectors shall be developed taking into account the severity of the effect of the disruption or destruction of a particular infrastructure. They shall be adopted by [*one year after the entry into force of this Directive*] at the latest.

   The sectoral criteria shall be developed for priority sectors while taking into account the characteristics of individual critical infrastructure sectors and involving, as appropriate, relevant stakeholders. They shall be adopted for each priority sector at the latest one year following the designation as a priority sector.

2. The priority sectors to be used for the purposes of developing the criteria provided for in paragraph 1 shall be identified by the Commission on an annual basis from among those listed in Annex I.

---

22 **FI suggests that this term is to be defined only in the relevant article; Pres suggests discussing this definition together with the relevant article.**

23 **SK suggested replacing "*impact of loss or change*" by "*size of after-effects of loss, damage or destroyed infrastructure*"**

24 **SK suggested replacing "*will be exploited*" by " *will be misused*"**

25 **UK suggested replacing "*critical*" by "*sensitive*"**

26 **FI requested a definition of the notions "*owner*" and "*operator*".**
SE requested a definition of the notion "protection".
SK recommended to integrate into article 2 also definitions of "*security plan*", "*threats scenario*", "*sector*", and "*priority sector*"

Annex I may be amended in accordance with the procedure referred to in Article 11(3) in so far as this does not broaden the scope of this Directive.

3. Each Member State shall identify the critical infrastructures located within its territory as well as critical infrastructures outside its territory that may have an impact on it, which satisfy the criteria adopted pursuant to paragraphs 1 and 2.

Each Member State shall notify the Commission of the critical infrastructures thus identified at the latest one year after the adoption of the relevant criteria and thereafter on an ongoing basis.

Article 4
Designation of European Critical Infrastructure

1. On the basis of the notifications made pursuant to the second paragraph of Article 3(3) and any other information at its disposal, the Commission shall propose a list of critical infrastructures to be designated as European Critical Infrastructures.

2. The list of critical infrastructures designated as European Critical Infrastructure shall be adopted in accordance with the procedure referred to in Article 11(3).

The list may be amended in accordance with the procedure referred to in Article 11(3).

Article 5
Operator Security Plans

1. Each Member State shall require the owners/operators of each European Critical Infrastructure located on its territory to establish and update an Operator Security Plan and to review it at least every two years.

2. The Operator Security Plan shall identify the assets of the European Critical Infrastructure and establish relevant security solutions for their protection in accordance with Annex II. Sector specific requirements concerning the Operator Security Plan taking into account existing Community measures may be adopted in accordance with the procedure referred to in Article 11(3).

Acting in accordance with the procedure referred to in Article 11(2), the Commission may decide that compliance with measures applicable to specific sectors listed in Annex I satisfies the requirement to establish and update an Operator Security Plan.

3. The owner/operator of a European Critical Infrastructure shall submit the Operator Security Plan to the relevant Member State authority within one year following designation of the critical infrastructure as a European Critical Infrastructure.

Where sector specific requirements concerning the Operator Security Plan are adopted based on paragraph 2, the operator security plan shall only be submitted to

the relevant Member State authority within 1 year following the adoption of the sector specific requirements.

4. Each Member State shall set up a system ensuring adequate and regular supervision of the Operator Security Plans and their implementation based on the risk and threat assessments conducted pursuant to Article 7(1).

5. Compliance with Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security satisfies the requirement to establish an Operator Security Plan.

Article 6
Security Liaison Officers

1. Each Member State shall require the owners/operators of European Critical Infrastructures on their territory to designate a Security Liaison Officer as the point of contact for security related issues between the owner/operator of the infrastructure and the relevant critical infrastructure protection authorities in the Member State. The Security Liaison Officer shall be designated within one year following the designation of the critical infrastructure as a European Critical Infrastructure.

2. Each Member State shall communicate relevant information concerning identified risks and threats to the Security Liaison Officers of the European Critical Infrastructure concerned.

Article 7
Reporting

1. Each Member State shall conduct a risk and threat assessment in relation to ECI situated on their territory within one year following the designation of the critical infrastructure as an ECI.

2. Each Member State shall report to the Commission on a summary basis on the types of vulnerabilities, threats and risks encountered in each sector referred to in Annex I within 18 months following the adoption of the list provided for in Article 4(2) and thereafter on an ongoing basis every two years.

   A common template for these reports shall be developed in accordance with the procedure referred to in Article 11(3).

3. The Commission shall assess on a sectoral basis whether specific protection measures are required for European Critical Infrastructures.

4. Common methodologies for carrying out vulnerability, threat and risk assessments in respect of European Critical Infrastructures may be developed on a sectoral basis in accordance with the procedure referred to in Article 11(3).

Article 8
Commission support for ECI

The Commission shall support the owners/operators of designated European Critical Infrastructures by providing access to available best practices and methodologies related to critical infrastructure protection.

Article 9
CIP Contact Points

1. Each Member State shall appoint a critical infrastructure protection Contact Point.

2. The Contact Point shall coordinate critical infrastructure protection issues within the Member State, with other Member States and with the Commission.

Article 10
Confidentiality and CIP information exchange

1. In applying this Directive, the Commission shall take appropriate measures, in accordance with Decision 2001/844/EC, ECSC, Euratom, to protect information subject to the requirement of confidentiality to which it has access or which is communicated to it by Member States. Member States shall take equivalent measures in accordance with relevant national legislation. Due account shall be given to the gravity of the potential prejudice to the essential interests of the Community or of one or more of its Member States.

2. Any person handling confidential information pursuant to this Directive on behalf of a Member State shall have an appropriate level of security vetting by the Member State concerned.

3. Member States shall ensure that Critical Infrastructure Protection Information submitted to the Member States or to the Commission, is not used for any purpose other than the protection of critical infrastructures.

Article 11
Committee

1. The Commission shall be assisted by a Committee composed of a representative of each CIP Contact Point.

2. Where reference is made to this paragraph, Articles 3 and 7 of Decision 1999/468/EC shall apply having regard to the provisions of Article 8 thereof.

3. Where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

The period laid down in Article 5(6) of Decision 1999/468/EC shall be set at one month.

4. The Committee shall adopt its Rules of Procedure.

Article 12
Implementation

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 31 December 2007 at the latest. They shall forthwith communicate to the Commission the text of those provisions and a correlation table between those provisions and this Directive.

   When Member States adopt these provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 13
Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Article 14
Addressees

This Directive is addressed to all Member States.

Done at Brussels,

For the Council
The President

ANNEX I

LIST OF CRITICAL INFRASTRUCTURE SECTORS

Sector		Sub-sector	
I	Energy	1	Oil and gas production, refining, treatment, storage and distribution by pipelines
		2	Electricity generation and transmission
II	Nuclear industry	3	Production and storage/processing of nuclear substances
III	Information, Communication Technologies, ICT	4	Information system and network protection
		5	Instrumentation automation and control systems (SCADA etc.)
		6	Internet
		7	Provision of fixed telecommunications
		8	Provision of mobile telecommunications
		9	Radio communication and navigation
		10	Satellite communication
		11	Broadcasting
IV	Water	12	Provision of drinking water
		13	Control of water quality
		14	Stemming and control of water quantity
V	Food	15	Provision of food and safeguarding food safety and security
VI	Health	16	Medical and hospital care
		17	Medicines, serums, vaccines and pharmaceuticals
		18	Bio-laboratories and bio-agents
VII	Financial	19	Payment and securities clearing and settlement infrastructures and systems
		20	Regulated markets
VIII	Transport	21	Road transport
		22	Rail transport
		23	Air transport
		24	Inland waterways transport
		25	Ocean and short-sea shipping
IX	Chemical industry	26	Production and storage/processing of chemical substances
		27	Pipelines of dangerous goods (chemical substances)
X	Space	28	Space
XI	Research facilities	29	Research facilities

ANNEX II

OPERATOR SECURITY PLAN (OSP)

The OSP shall identify the critical infrastructure owners' and operators' assets and establish relevant security solutions for their protection. The OSP will cover at least:

– 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.