COUNCIL OF THE EUROPEAN UNION

Brussels, 22 May 2008

9403/08

LIMITE

JAI 240
PROCIV 63
COTER 28
ENER 141
TRANS 147
TELECOM 69
ATO 39
ECOFIN 177
ENV 292
SAN 80
CHIMIE 24
RECH 176
DENLEG 50
RELEX 308

NOTE

From:	General Secretariat
To:	Delegations
Subject:	Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection

For the purpose of achieving political agreement at the Justice and Home Affairs Council on 5.6. June 2008, delegations will find attached a draft Directive on the above subject, as agreed at Working Party level.

ANNEX 1

Directive

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

(Text with EEA relevance)

OF THE EUROPEAN UNION,

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

Having regard to the proposal from the Commission[1],

Having regard to the opinion of the European Parliament[2],

[1] OJ C […], […], p. […].

[2] OJ C […], […], p. […].

Whereas:

(1) In June 2004, the European Council asked for the preparation of an overall strategy to protect critical infrastructures[3]. In response, on 20 October 2004, the Commission adopted a Communication on Critical Infrastructure Protection in the Fight against Terrorism[4] which put forward suggestions as to what would enhance European prevention of, preparedness for and response to terrorist attacks involving critical infrastructures.

(2) On 17 November 2005 the Commission adopted a Green Paper on a European Programme for Critical Infrastructure Protection[5] 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 emphasised the added value of 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 key principles of subsidiarity, proportionality and complementarity, as well as 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.

---

3 10679/2/04 REV 2.
4 13979/04
5 14910/05

(4) In April 2007 the Council adopted conclusions on the European Programme for Critical Infrastructure Protection in which it reiterated that it was the ultimate responsibility of the Member States to manage arrangements for the protection of critical infrastructures within their national borders while welcoming the efforts of the Commission to develop a European procedure for the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection.

(4a) This Directive constitutes a first step in a step-by-step approach to identify and designate European Critical Infrastructure and assess the need to improve their protection. As such, this Directive concentrates on the energy and transport sector, and will be reviewed with a view to assessing its impact and the need to include other sectors within its scope, inter alia the Information and Communication Technology (ICT) sector.

(5) The primary and ultimate responsibility for protecting European Critical Infrastructure falls on the Member States and the owners/operators of such infrastructures.

(6) There are a certain number of critical infrastructures in the Community, the disruption or destruction of which would have significant cross-border impacts. This may include transboundary cross-sector effects resulting from interdependencies between interconnected infrastructures. Such European critical infrastructures should be identified and designated by means of a common procedure. The evaluation of security requirements for such infrastructure should be done under a common minimum approach. 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. Information pertaining to the designation of a particular infrastructure as a European Critical Infrastructure should be classified at an appropriate level in accordance with existing Community and Member State legislation.

(7) 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.

(8) In terms of the energy sector and in particular the methods of electricity generation and transmission (in respect of supply of electricity), it is understood that where deemed appropriate, electricity generation may include electricity transmission parts of nuclear power plants, but exclude the specifically nuclear elements covered by relevant nuclear legislation including nuclear treaties and Community law.

(9) 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. Duplication of, or contradiction between, different acts or provisions shall be avoided.

(10) Operator Security Plans or equivalent measures comprising an identification of important assets, a risk assessment and the identification, selection and prioritisation of counter-measures and procedures should be in place in all designated European Critical Infrastructure. With a view to avoiding unnecessary work and duplication, each Member State should first assess whether the owners/operators of designated European Critical Infrastructure possess relevant Operator Security Plans or similar measures. Where such plans do not exist, each Member State should take the necessary steps to make sure that appropriate measures are put in place. It is up to each Member State to decide on the most appropriate form of action with regard to the establishment of Operator Security Plans.

(11) Measures, principles, guidelines including Community measures as well as bilateral and/or multilateral cooperation schemes that provide for a plan similar or equivalent to an Operator Security Plan or provide for a Security Liaison Officer or equivalent, should be deemed to satisfy the requirements of this Directive in relation to the Operator Security Plan or the Security Liaison Officer respectively.

(12) Security Liaison Officers should be identified in all designated European Critical Infrastructure in order to facilitate cooperation and communication with relevant national critical infrastructure protection authorities. With a view to avoiding unnecessary work and duplication, each Member State should first assess whether the owners/operators of designated European Critical Infrastructure already possess a Security Liaison Officer or equivalent.

Where such a Security Liaison Officer does not exist, each Member State should take the necessary steps to make sure that appropriate measures are put in place. It is up to each Member State to decide on the most appropriate form of action with regard to the designation of Security Liaison Officers.

(13) 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 in sectors where the European Critical Infrastructure was identified, including where relevant information on possible improvements in the European Critical Infrastructures and cross-sector dependencies, which could be the basis for the development of specific proposals by the Commission on improving the protection of European Critical Infrastructure, where necessary.

(14) In order to facilitate improvements in the protection of European Critical Infrastructures, common methodologies may be developed for the identification and classification of vulnerabilities, threats and risks to infrastructure assets.

(15) Owners/operators of European Critical Infrastructure should be given access primarily through relevant Member State authorities to best practices and methodologies concerning critical infrastructure protection.

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

(17) In order to develop European 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. It is important that the rules of confidentiality according to applicable national law or the Regulation (EC) No. 1049/2001 regarding public access to European Parliament, Council and Commission documents are observed with regard to specific facts about critical infrastructure assets, which could be used to plan and act with a view to causing unacceptable consequences for critical infrastructure installations. Classified information should be protected in accordance with relevant Community and Member State legislation. Each Member State and the Commission should respect the relevant security classification given by the originator of a document.

(18) Information sharing regarding European 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 and confidential data will be sufficiently protected.

(19) 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.

(20) 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.

Article 2

Definitions

For the purpose of this Directive:

a) “Critical Infrastructure” means those assets, systems or parts thereof located in the EU 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;

b) “European Critical Infrastructure” means critical infrastructure located in the EU Member States the disruption or destruction of which would have a significant impact on at least two Member States of the EU. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure;

c) "risk analysis" means consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure.

d) "Sensitive Critical Infrastructure Protection related Information” means facts about a critical infrastructure, which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations.

e) "protection" means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructure in order to deter, mitigate and neutralise a threat, risk or vulnerability.

f) "European Critical Infrastructure owners/operators" means those entities responsible for investments or day-to-day operation and investment in a particular asset, system or part thereof designated as a European Critical Infrastructure under this Directive.

Article 3

Identification of European Critical Infrastructure

1. Pursuant to the procedure provided in Annex III, each Member State shall identify the potential European Critical Infrastructure which both satisfy the cross-cutting and sectoral criteria and meet the definitions set out in Article 2(a) and 2(b).

   The Commission may assist Member States at their request to identify potential European Critical Infrastructure.

   The Commission may draw the attention of the relevant Member States to the existence of potential critical infrastructure which may be deemed to satisfy the requirements for designation as a European Critical Infrastructure.

   Each Member State and the Commission will continue on an ongoing basis the process of identifying potential European Critical Infrastructure.

2. The cross-cutting criteria shall comprise the following:

   - Casualties criterion (assessed in terms of the 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 on public confidence, physical suffering and disruption of daily life; including the loss of essential services).

The cross-cutting criteria thresholds shall be based on the severity of the impact of the disruption or destruction of a particular infrastructure. The precise thresholds applicable to the cross-cutting criteria shall be determined on a case-by-case basis by the Member States concerned by a particular critical infrastructure. Each Member State shall inform the Commission on an annual basis of the number of infrastructures per sector for which discussions were held concerning the cross-cutting criteria thresholds.

The sectoral criteria shall take into account the characteristics of individual European Critical Infrastructure sectors.

The Commission together with the Member States shall develop guidelines for the application of the cross-cutting and sectoral criteria and approximate thresholds to be used to identify European Critical Infrastructure. The criteria shall be classified. The use of such guidelines will be optional for the Member States.

3. The sectors to be used for the purposes of implementing this Directive shall be the energy and transport sectors. The sub-sectors are identified in Annex I.

If deemed appropriate and in conjunction with the review of this Directive as laid down in Article 11, subsequent sectors to be used for the purpose of implementing this Directive may be identified. Priority should be given to the Information and Communication Technology (ICT) sector.

Article 4

Designation of European Critical Infrastructure

1. Each Member State shall inform the other Member States which may be significantly affected by a potential European Critical Infrastructure about its identity and the reasons for designating it as a potential European Critical Infrastructure.

2. Each Member State on whose territory a potential European Critical Infrastructure is located shall engage in bilateral and/or multilateral discussions with the other Member States which may be significantly affected by the potential European Critical Infrastructure. The Commission may participate in these discussions but will not have access to detailed information which would allow for the unequivocal identification of a particular infrastructure.

   A Member State that has reason to believe that it may be significantly affected by the potential European Critical Infrastructure, but has not been identified as such by the Member State on whose territory the potential European Critical Infrastructure is located, may inform the Commission about its wish to be engaged in bilateral and/or multilateral discussions on this issue. The Commission shall without delay communicate this wish to the Member State on whose territory the potential European Critical Infrastructure is located and endeavour to facilitate agreement between the parties.

3. The Member State on whose territory a potential European Critical Infrastructure is located shall designate it as a European Critical Infrastructure following an agreement between that Member State and those Member States that may be significantly affected.

   The acceptance of the Member State on whose territory the infrastructure to be designated as a European Critical Infrastructure is located, shall be required.

4. The Member State on whose territory a designated European Critical Infrastructure is located shall inform the Commission on an annual basis of the number of designated European Critical Infrastructure per sector and of the number of Member States dependent on each designated European Critical Infrastructure. Only those Member States that may be significantly affected by a European Critical Infrastructure shall know its identity.

5. The Member States on whose territory the European Critical Infrastructure is located shall inform the owner/operator of the infrastructure concerning its designation as a European Critical Infrastructure. Information concerning the designation of an infrastructure as a European Critical Infrastructure shall be classified at an appropriate level.

6. The process of identifying and designating European Critical Infrastructure pursuant to Articles 3 and 4 of this Directive shall be completed within 24 months of the entry into force of this Directive and reviewed on a regular basis.

Article 5

Operator Security Plans

1. The Operator Security Plan procedure shall identify the critical infrastructure assets of the European Critical Infrastructure and which security solutions exist or are being implemented for their protection. The minimum content to be addressed by an Operator Security Plan procedure is set out in Annex II.

2. Each Member State shall assess whether each designated European Critical Infrastructure located on its territory possesses an Operator Security Plan or has in place equivalent measures addressing the issues identified in Annex II. If a Member State finds that such an Operator Security Plan or equivalent exists and is updated regularly, no further implementation action shall be necessary.

3. If a Member State finds that such an Operator Security Plan or equivalent has not been prepared, it shall ensure by any measures deemed appropriate, that the Operator Security Plan or equivalent is prepared addressing the issues identified in Annex II.

   Each Member State shall ensure that the Operator Security Plans or equivalent are in place and are reviewed regularly within one year following designation of the critical infrastructure as a European Critical Infrastructure. This period may be extended in exceptional circumstances, by agreement with the Member State authority and with a notification to the Commission.

4. In a case where supervisory or oversight arrangements already exist in relation to a European Critical Infrastructure such arrangements are not affected by this Article and the relevant Member State authority referred to in this Article shall be the supervisor under those existing arrangements.

5. Compliance with measures including Community measures which in a particular sector require, or refer to a need to have, a plan similar or equivalent to an Operator Security Plan and oversight by the relevant authority of such a plan, is deemed to satisfy all the requirements of Member States in, or adopted pursuant to, this Article. The guidelines for implementation referred to in article 3(2) shall contain an indicative list of such measures.

Article 6

Security Liaison Officers

1. The Security Liaison officer shall function as the point of contact for security related issues between the owner/operator of the European Critical Infrastructure and the relevant Member State authority.

2. Each Member State shall assess whether each designated European Critical Infrastructure located on its territory possesses a Security Liaison Officer or equivalent. If a Member State finds that such a Security Liaison Officer is in place or an equivalent exists, no further implementation action shall be necessary.

3. If a Member State finds that a Security Liaison Officer or equivalent does not exist in relation to a designated European Critical Infrastructure, it shall ensure by any measures deemed appropriate, that such a Security Liaison Officer or equivalent is designated.

4. Each Member State shall implement an appropriate communication mechanism between the relevant Member State authority and the Security Liaison Officer or equivalent with the objective of exchanging relevant information concerning identified risks and threats in relation to the European Critical Infrastructure concerned. This communication mechanism shall be without prejudice to national requirements concerning access to sensitive and classified information.

5. Compliance with measures including Community measures which in a particular sector require, or refer to a need to have, a Security Liaison Officer or equivalent, is deemed to satisfy all the requirements of Member States in, or adopted pursuant to, this Article. The guidelines for implementation referred to in article 3(2) shall contain an indicative list of such measures.

Article 7

Reporting

1. Each Member State shall conduct a threat assessment in relation to European Critical Infrastructure sub-sectors within one year following the designation of critical infrastructure on its territory as European Critical Infrastructure within those sub-sectors.

2. Each Member State shall report every 24 months to the Commission generic data on a summary basis on the types of vulnerabilities, threats and risks encountered per European Critical Infrastructure sector in which European Critical Infrastructure have been identified pursuant to Article 4 and are located on its territory.

   A common template for these reports may be developed by the Commission in cooperation with the Member States.

   Each report shall be classified at an appropriate level as deemed necessary by the originating Member State.

3. Based on the reports referred to in paragraph 2, the Commission and the Member States shall assess on a sectoral basis whether further protection measures at the EU level should be considered for European Critical Infrastructure. This process shall be undertaken in conjunction with the review of this Directive as laid down in Article 11.

4. Common methodological guidelines for carrying out risk analyses in respect of European Critical Infrastructures may be developed by the Commission in cooperation with the Member States. The use of such guidelines will be optional for the Member States.

Article 8

Commission support for European Critical Infrastructure

The Commission shall support, through the relevant Member State authority, the owners/operators of designated European Critical Infrastructures by providing access to available best practices and methodologies as well as support training and the exchange of information on new technical developments related to critical infrastructure protection.

Article 9

Sensitive European Critical Infrastructure Protection -related Information

1. Any person handling classified information pursuant to this Directive on behalf of a Member State or the Commission shall have an appropriate level of security vetting.

   Member States, the Commission, and relevant supervisory bodies shall ensure that sensitive European Critical Infrastructure Protection - related information submitted to the Member States or to the Commission, is not used for any purpose other than the protection of critical infrastructures.

2. The provisions of this Article shall also apply to non-written information exchanged during meetings at which sensitive subjects are discussed.

Article 10

European Critical Infrastructure Protection Contact Points

1. Each Member State shall appoint a European Critical Infrastructure Protection - Contact Point ("European CIP Contact Points").

2. The Contact Point shall coordinate European Critical Infrastructure Protection issues within the Member State, with other Member States and with the Commission. The appointment of a European CIP Contact Point does not preclude other authorities in a Member State from being involved in European Critical Infrastructure Protection issues.

Article 11

Review

This Directive shall be reviewed in three years following its entry into force.

Article 12

Implementation

Member States shall take the necessary measures to comply with this Directive at the latest two years after its entry into force. They shall forthwith inform the Commission thereof and communicate the text of those measures and their correlation with this Directive.

When Member States adopt these measures, 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.

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

LIST OF EUROPEAN CRITICAL INFRASTRUCTURE SECTORS

Sector		Sub-sector	
I	Energy	1. Electricity	Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity
		2. Oil	Oil production, refining, treatment, storage and transmission by pipelines
		3. Gas	Gas production, refining, treatment, storage and transmission by pipelines LNG terminals
II	Transport	4. Road transport 5. Rail transport 6. Air transport 7. Inland waterways transport 8. Ocean and short-sea shipping and ports	

The identification by the Member States of critical infrastructure which may be designated as European Critical Infrastructure is done pursuant to article 3. Therefore the list of European critical infrastructure sectors in itself does not generate a generic obligation to designate a European Critical Infrastructure in each sector.

OPERATOR SECURITY PLAN (OSP) PROCEDURE

The OSP shall identify critical infrastructure assets and which security solutions exist or are being implemented for their protection. The OSP procedure 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 are relevant to be employed at all times. This heading will include information concerning general measures such as 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 can be activated according to varying risk and threat levels.

Procedure for the identification by the Member States of Critical Infrastructure which may be designated as European Critical Infrastructure pursuant to Article 3

Article 3 of this Directive requires each Member State to identify the critical infrastructure which may be designated as European Critical Infrastructure. This procedure shall be implemented by each Member State through the following series of consecutive steps.
Potential European Critical Infrastructure (ECI) which does not satisfy the requirements of one of the following sequential steps is considered to be 'non-ECI' and is excluded from the procedure. Potential European Critical Infrastructure which does satisfy the definitions shall be subjected to the next steps of this procedure.

Step 1
Each Member State shall apply the sectoral criteria in order to make a first selection of critical infrastructures within a sector.

Step 2
Each Member State shall apply the definition of critical infrastructure pursuant to Article 2(a) to the potential European Critical Infrastructure identified under step 1.
The significance of the impact will be determined either by using national methods for identifying critical infrastructures or with reference to the cross-cutting criteria, at an appropriate national level. For infrastructure providing an essential service, the availability of alternatives, and the duration of disruption/recovery will be taken into account.

Step 3
Each Member State shall apply the definition of European Critical Infrastructure pursuant to Article 2(b) to the potential European Critical Infrastructure that has passed the first two steps of this procedure. Potential European Critical Infrastructure which does satisfy the definition will follow the next step of the procedure. For infrastructure providing an essential service, the availability of alternatives, and the duration of disruption/recovery will be taken into account.

Step 4

Each Member State shall apply the cross-cutting criteria to the remaining potential European Critical Infrastructure. The cross-cutting criteria shall take into account: the severity of impact; and, for infrastructure providing an essential service, the availability of alternatives; and the duration of disruption/recovery. Potential European Critical Infrastructure which does not satisfy the cross-cutting criteria will not be considered to be European Critical Infrastructure.

Potential European Critical Infrastructure which has passed through this procedure shall only be communicated to the Member States which may be significantly affected by the potential European Critical Infrastructure.

_____