COUNCIL DIRECTIVE 2008/114/EC

of 8 December 2008

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

(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 proposal from the Commission,

Having regard to the opinion of the European Parliament [1],

Having regard to the opinion of the European Central Bank [2],

Whereas:

(1) In June 2004 the European Council asked for the preparation of an overall strategy to protect critical infrastructures. In response, on 20 October 2004, the Commission adopted a Communication on critical infrastructure protection in the fight against terrorism 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 which provided policy options on the establishment of the programme and the Critical Infrastructure Warning Information Network. 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, man-made, 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.

(4) In April 2007 the Council adopted conclusions on the EPCIP 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 infrastructures ('ECIs') and the assessment of the need to improve their protection.

(5) This Directive constitutes a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection. As such, this Directive concentrates on the energy and transport sectors and should 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.

(6) The primary and ultimate responsibility for protecting ECIs falls on the Member States and the owners/operators of such infrastructures.

(7) 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 ECIs should be identified and designated by means of a common procedure. The evaluation of security requirements for such infrastructures 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 infrastructures. EPCIP should build on such cooperation. Information pertaining to the designation of a particular infrastructure as an ECI should be classified at an appropriate level in accordance with existing Community and Member State legislation.

[1] Opinion of 10 July 2007 (not yet published in the Official Journal).
[2] OJ C 116, 26.5.2007, p. 1.

(8) 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 Community, national or regional level, and where relevant cross-border mutual aid agreements between owners/operators of critical infrastructures 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 needs to encourage full private sector involvement.

(9) 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 treaties and Community law.

(10) 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 should be avoided.

(11) Operator security plans ('OSPs') 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 ECIs. With a view to avoiding unnecessary work and duplication, each Member State should first assess whether the owners/operators of designated ECIs possess relevant OSPs 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 OSPs.

(12) 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 OSP or provide for a Security Liaison Officer or equivalent, should be deemed to satisfy the requirements of this Directive in relation to the OSP or the Security Liaison Officer respectively.

(13) Security Liaison Officers should be identified for all designated ECIs 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 ECIs 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.

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

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

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

(17) Effective protection of ECIs requires communication, coordination, and cooperation at national and Community level. This is best achieved through the nomination of European critical infrastructure protection contact points ('ECIP 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.

(18) 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 Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents [1] 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.

(19) Information sharing regarding ECIs 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.

(20) Since the objectives of this Directive, namely the creation of a procedure for the identification and designation of ECIs, and a common approach to the assessment of the need 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.

(21) 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 ('ECIs'), and a common approach to the assessment of the need 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 an asset, system or part thereof located in Member States which is 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' or 'ECI' means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. 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 infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability;

(f) 'owners/operators of ECIs' means those entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part thereof designated as an ECI under this Directive.

Article 3

Identification of ECIs

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

[1] OJ L 145, 31.5.2001, p. 43.

The Commission may assist Member States at their request to identify potential ECIs.

The Commission may draw the attention of the relevant Member States to the existence of potential critical infrastructures which may be deemed to satisfy the requirements for designation as an ECI.

Each Member State and the Commission shall continue on an ongoing basis the process of identifying potential ECIs.

2. The cross-cutting criteria referred to in paragraph 1 shall comprise the following:

(a) casualties criterion (assessed in terms of the potential number of fatalities or injuries);

(b) economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects);

(c) 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 ECI 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 ECIs. The criteria shall be classified. The use of such guidelines shall 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 subsectors 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 shall be given to the ICT sector.

Article 4

Designation of ECIs

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

2. Each Member State on whose territory a potential ECI is located shall engage in bilateral and/or multilateral discussions with the other Member States which may be significantly affected by the potential ECI. The Commission may participate in these discussions but shall 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 ECI, but has not been identified as such by the Member State on whose territory the potential ECI 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 ECI is located and endeavour to facilitate agreement between the parties.

3. The Member State on whose territory a potential ECI is located shall designate it as an ECI 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 an ECI is located, shall be required.

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

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

6. The process of identifying and designating ECIs pursuant to Article 3 and this Article shall be completed by 12 January 2011 and reviewed on a regular basis.

Article 5

Operator security plans

1. The operator security plan ('OSP') procedure shall identify the critical infrastructure assets of the ECI and which security solutions exist or are being implemented for their protection. The minimum content to be addressed by an ECI OSP procedure is set out in Annex II.

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

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

Each Member State shall ensure that the OSP or equivalent is in place and is reviewed regularly within one year following designation of the critical infrastructure as an ECI. 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 an ECI 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 OSP and oversight by the relevant authority of such a plan, is deemed to satisfy all the requirements of Member States under, or adopted pursuant to, this Article. The guidelines for application 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 ECI and the relevant Member State authority.

2. Each Member State shall assess whether each designated ECI 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 ECI, 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 ECI 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 application 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 ECI subsectors within one year following the designation of critical infrastructure on its territory as an ECI within those subsectors.

2. Each Member State shall report every two years to the Commission generic data on a summary basis on the types of risks, threats and vulnerabilities encountered per ECI sector in which an ECI has been designated pursuant to Article 4 and is 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 Community level should be considered for ECIs. 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 ECIs may be developed by the Commission in cooperation with the Member States. The use of such guidelines shall be optional for the Member States.

Article 8

Commission support for ECIs

The Commission shall support, through the relevant Member State authority, the owners/operators of designated ECIs 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. 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 ('ECIP contact point').

2. ECIP contact points shall coordinate European critical infrastructure protection issues within the Member State, with other Member States and with the Commission. The appointment of an ECIP contact point does not preclude other authorities in a Member State from being involved in European critical infrastructure protection issues.

Article 11

Review

A review of this Directive shall begin on 12 January 2012.

Article 12

Implementation

Member States shall take the necessary measures to comply with this Directive by 12 January 2011. They shall forthwith inform the Commission thereof and communicate the text of those measures and their correlation with this Directive.

When they are adopted by Member States, these measures shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

Article 13

Entry into force

This Directive shall enter into force on the 20th day following its publication in the *Official Journal of the European Union*.

Article 14

Addressees

This Directive is addressed to the Member States.

Done at Brussels, 8 December 2008.

For the Council

The President

B. KOUCHNER

ANNEX I

List of ECI sectors

Sector	Subsector	
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 infrastructures which may be designated as ECIs is undertaken pursuant to Article 3. Therefore the list of ECI sectors in itself does not generate a generic obligation to designate an ECI in each sector.

ANNEX II

ECI OSP PROCEDURE

The OSP will identify critical infrastructure assets and which security solutions exist or are being implemented for their protection. The ECI OSP procedure will cover at least:

1. identification of important assets;

2. conducting a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact; and

3. 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); organisational 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.

ANNEX III

Procedure for the identification by the Member States of critical infrastructures which may be designated as an ECI pursuant to Article 3

Article 3 requires each Member State to identify the critical infrastructures which may be designated as an ECI. This procedure shall be implemented by each Member State through the following series of consecutive steps.

A potential 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. A potential ECI which does satisfy the requirements 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 ECI 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 transboundary element of the definition of ECI pursuant to Article 2(b) to the potential ECI that has passed the first two steps of this procedure. A potential ECI 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 ECIs. 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. A potential ECI which does not satisfy the cross-cutting criteria will not be considered to be an ECI.

A potential ECI which has passed through this procedure shall only be communicated to the Member States which may be significantly affected by the potential ECI.