COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 12.12.2006
COM(2006) 787 final

2006/0276 (CNS)

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

(presented by the Commission)

{SEC(2006) 1648}
{SEC(2006) 1654}

EXPLANATORY MEMORANDUM

1) CONTEXT OF THE PROPOSAL

- **Grounds for and objectives of the proposal**

The European Council of June 2004 asked the Commission to prepare an overall strategy to protect critical infrastructure. The Commission adopted on 20 October 2004 a Communication on Critical Infrastructure Protection in the Fight against Terrorism which put forward suggestions on what would enhance European prevention, preparedness and response to terrorist attacks involving critical Infrastructures (CI).

The Council conclusions on "Prevention, Preparedness and Response to Terrorist Attacks" and the "EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks" adopted by Council in December 2004 endorsed the intention of the Commission to propose a European Programme for Critical Infrastructure Protection (EPCIP) and agreed to the set-up by the Commission of a Critical Infrastructure Warning Information Network (CIWIN).

In November 2005, the Commission adopted a Green Paper on a European Programme for Critical Infrastructure Protection (EPCIP) which provided policy options on how the Commission could establish EPCIP and CIWIN.

In December 2005 the Justice and Home Affairs (JHA) Council called upon the Commission to make a proposal on EPCIP by June 2006.

This proposal for a Directive presents the measures that the Commission is proposing on the identification and designation of European Critical Infrastructures (ECI) and the assessment of the need to improve their protection.

- **General context**

There exist a number of critical infrastructures in the European Union, which if disrupted or destroyed, would affect two or more Member States. It may also happen that failure of a critical infrastructure in one Member State causes effects in another Member State. Such critical infrastructures with a trans-national dimension should be identified and designated as European Critical Infrastructures (ECI). This can only be done through a common procedure concerning ECI identification and the assessment of the need to improve their protection.

Because of the trans-national dimension, when investigating the weaknesses and vulnerabilities and identifying gaps in protective measures, an integrated EU-wide approach would usefully complement and add value to the national programmes for critical infrastructure protection already in place in the Member States and would add important value to the continued viability and wealth creation capabilities of the European internal market.

Since various sectors possess particular experience, expertise and requirements concerning critical infrastructure protection (CIP), an EU approach to CIP should be developed and implemented taking into account critical infrastructure (CI) sector specificities and should be built on existing CI sector-based measures. The establishment of a common list of critical infrastructure sectors is needed in order to facilitate the implementation of the sector-by-sector approach to critical infrastructure protection.

- **The need for a common framework**

Only a common framework can provide the necessary basis for a coherent and uniform implementation of measures to enhance the protection of ECI, as well as defining clearly the respective responsibilities of ECI stakeholders. Non-binding voluntary measures, while flexible, would not provide the necessary stable foundation as they would not provide enough clarity on who does what, nor would they clarify the rights and obligations for ECI stakeholders involved.

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 can only be established by way of a directive in order to ensure:

- adequate levels of protection concerning ECI;
- all ECI stakeholders are subjected to similar rights and obligations;
- the stability of the Internal Market is maintained.

The damage or loss of a piece of infrastructure in one MS may have negative effects on several others and on the European economy as a whole. This is becoming increasingly likely as new technologies (e.g. the Internet) and market liberalisation (e.g. in electricity and gas supply) mean that much infrastructure is part of a larger network. In such a situation protection measures are only as strong as their weakest link. This means that a common level of protection may be necessary.

- **A sector dialogue with stakeholders**

Effective protection requires communication, coordination, and cooperation nationally and at EU level involving all relevant stakeholders.

Full involvement of the private sector is important as most critical infrastructure is privately owned and operated. Each operator needs to control the management of their risks as it is normally the operator's sole decision which protection measures and business continuity plans to implement. Continuity planning should respect normal business processes and logic and where possible solutions should be based on standard commercial arrangements.

Sectors possess particular experience, expertise and requirements concerning the protection of their critical infrastructure.

Hence, in line with the responses to the EPCIP Green Paper the EU approach should fully involve the private sector, taking into account sector characteristics and should be built on existing sector-based protection measures.

- **Existing provisions in the area of the proposal**

No horizontal provisions on critical infrastructure protection currently exist at EU level. 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.

A number of sectoral measures exist including:

- In the IT sector:

  (a) Universal Service Directive (2002/22/EC) which deals inter alia with the integrity of public electronic communications networks

  (b) Authorisation Directive (2002/20/EC) which deals inter alia with the integrity of public electronic communications networks

  (c) E Privacy Directive (2002/58/EC) which deals inter alia with the security of public electronic communications networks

  (d) Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

  (e) Regulation (EC) No 460/2004 of 10 March 2004 establishing the European Network and Information security Agency ENISA

- In the health sector:

  (a) Decision No 2119/98/EC of the European Parliament and of the Council of 24 September 1998 setting up a network for the epidemiological surveillance and control of communicable diseases in the Community

  (b) Commission Directive 2003/94/EC of 8 October 2003 laying down the principles and guidelines of good manufacturing practice in respect of medicinal products for human use and investigational medicinal products for human use

- In the financial sector:

  (a) Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments (MiFID)

  (b) Oversight standards for euro retail payment systems adopted in June 2003 by the Governing Council of the European Central Bank (ECB)

  (c) Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 on the taking up and pursuit of the business of credit institutions

  (d) Directive 2006/49/EC of the European Parliament and of the Council of 14 June 2006 on the capital adequacy of investment firms and of credit institutions

  (e) Proposal for a Directive on payment services in the internal market amending Directive 97/7/EC, 2000/12/EC and 2002/65/EC (COM(2005) 603)

(f) Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions

(g) Directive 1998/26/EC of the European Parliament and of the Council of 19 May 1998 on Settlement Finality.

- In the transport sector:

(a) Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security

(b) Commission Regulation (EC) No 884/2005 of 10 June 2005 laying down procedures for conducting Commission inspections in the field of maritime security

(c) Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security

(d) Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security

(e) Regulation (CE) No 622/2003 of the Commission of 4 April 2003 laying down measures for the implementation of the common basic standards on aviation security

(f) Commission Regulation (EC) No 1217/2003 of 4 July 2003 laying down common specifications for national civil aviation security quality control programmes

(g) Commission Regulation (EC) No 1486/2003 of 22 August 2003 laying down procedures for conducting Commission inspections in the field of civil aviation security

(h) Commission Regulation (EC) No 68/2004 of 15 January 2004 amending Commission Regulation (EC) No 622/2003 laying down measures for the implementation of the common basic standards on aviation security

(i) Regulation (EC) No 849/2004 of the European Parliament and of the Council of 29 April 2004 amending Regulation (EC) No 2320/2002 establishing common rules in the field of civil aviation security

(j) Commission Regulation (EC) No 1138/2004 of 21 June 2004 establishing a common definition of critical parts of security restricted areas at airports

(k) Commission Regulation (EC) No 781/2005 of 24 May 2005 amending Regulation (EC) No 622/2003 laying down measures for the implementation of the common basic standards on aviation security

(l) Commission Regulation (EC) No 857/2005 of 6 June 2005 amending Regulation (EC) No 622/2003 laying down measures for the implementation of the common basic standards on aviation security

(m) Directive 2001/14/EC on the allocation of railway infrastructure capacity

(n) The transport of Dangerous Goods by rail is covered by D Directive. 1996/49/EC (amended by Directive 2004/110/EC, adopting RID 2005)

(o) Convention on the Physical Protection of Nuclear Materials (signed in 1980, acceded to in 1981 and entered into force in 1987)

- In the chemical sector:

(a) Hazardous Installations under the Seveso-II-Directive (Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances, "Seveso II Directive") amended by Directive 2003/105/EC of the European Parliament and of the Council of 16 December 2003

- In the nuclear sector:

(a) Council Directive 89/618/Euratom of 27 November 1989 on informing the general public about health protection measures to be applied and steps to be taken in the event of a radiological emergency

(b) Council Decision 87/600/Euratom of 14 December 1987 on Community arrangements for the early exchange of information in the event of a radiological emergency

- **Consistency with other policies and objectives of the Union**

This proposal is fully consistent with the objectives of the Union and specifically with the objective "to maintain and develop the Union as an area of freedom, security and justice, in which the free movement of persons is assured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime".

This proposal is consistent with other policies as it does not aim to replace existing measures, but to complement them in order to improve the protection of ECI.

2) CONSULTATION OF INTERESTED PARTIES AND IMPACT ASSESSMENT

- **Consultation of interested parties**

All relevant stakeholders have been consulted concerning the development of EPCIP. This has been done through:

- The EPCIP Green Paper adopted in on 17 November 2005 with the consultation period ending on 15 January 2006. 22 Member States provided official responses to the consultation. Around 100 private sector representatives also provided comments to the Green Paper. The responses were generally supportive of the idea of creating EPCIP.

- Three Critical Infrastructure Protection seminars hosted by the Commission (in June 2005, September 2005 and March 2006). All three seminars brought together representatives of the Member States. The private sector was invited to the seminars held in September 2005 and March 2006.

- Informal meetings of CIP Contact Points. The Commission hosted two meetings of the CIP Contact Points of the Member States (December 2005 and February 2006).

- Informal meetings with private sector representatives. Numerous informal meetings were held with representatives of particular private business as well as with industry associations.

- Internally, within the Commission, work on the development of EPCIP was taken forward with the help of regular meeting of the sub-group on Critical Infrastructure Protection on the Inter-Service Group on the Internal Aspects of Terrorism.

- **Collection and use of expertise**

Available expertise was collected through numerous meetings and seminars held in 2004, 2005 and 2006, as well as through the EPCIP Green Paper consultation process. Information was collected from all relevant stakeholders.

- **Impact assessment**

A copy of the EPCIP Impact Assessment is attached.

3) LEGAL ELEMENTS OF THE PROPOSAL

- **Summary of the proposed action**

The proposed action creates a horizontal framework for the identification and designation of European Critical Infrastructures and for the assessment of needs to improve their protection.

- **Legal basis**

The legal basis for the proposal is Article 308 of the Treaty establishing the European Community.

- **Subsidiarity principle**

The subsidiarity principle is satisfied as the measures being undertaken through this proposal cannot be achieved by any single EU Member State and must therefore be addressed at EU level. Although it is the responsibility of each Member State to protect the critical

infrastructure under its jurisdiction, it is crucial for the security of the European Union to make sure that infrastructure having an impact on two or more Member States or a single Member State if the critical infrastructure is located in another Member State are sufficiently protected and that one or more Member States are not made vulnerable by weaknesses or lower security standards in other Member States. Similar rules concerning security would also help to make sure that the rules of competition within the internal market are not distorted.

- **Proportionality principle**

This proposal does not go beyond what is necessary in order to achieve the underlying objectives of improving the protection of European critical infrastructure. The key ideas put forward by the proposal include the creation of a basic EU level coordination mechanism, putting an obligation on the Member States to identify their critical infrastructures, implementation of a set of basic security measures for critical infrastructures and finally the identification and designation of key European critical infrastructures. The proposal therefore puts forward the minimal number of requirements needed to begin work to improve the protection of critical infrastructures. This objective cannot be sufficiently achieved through other measures, namely by adopting a guideline approach to EPCIP, as this would not ultimately ensure improved levels of protection across the entire EU and the full participation of all stakeholders.

- **Choice of instruments**

The Member States have varying approaches to critical infrastructure protection and different legal systems. A directive is therefore best suited to create a common 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.

4) BUDGETARY IMPLICATION

The budgetary impact is estimated in the accompanying financial statement.

The programme " Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013 will contribute to the implementation of this directive in the protection of people against security risks and those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the critical societal functions as part of the general programme entitled "Security and safeguarding liberties".

This programme does not apply to matters that are covered by other financial instruments and in particular by the Rapid Response Instrument in the event of major emergencies, and the EU Solidarity Fund.

5) ADDITIONAL INFORMATION

- **Repeal of existing legislation**

No existing legislation has to be repealed.

- **Detailed explanation of the proposal**

Article 1 – the subject-matter of the Directive is presented. The Directive establishes a common procedure for the identification and designation of European Critical Infrastructures, meaning those infrastructures, the destruction or disruption of which would affect two or more MS, or a single Member State if the critical infrastructure is located in another Member State. The Directive also introduces a common approach to the assessment of the needs to improve the protection of European Critical Infrastructures. This assessment will help prepare specific protection measures in the individual CIP sectors.

Article 2 – a list of basic definitions pertinent to the Directive is presented.

Article 3 – the procedure for the identification of ECI is presented. ECI means those critical infrastructures the disruption or destruction of which would have a serious impact on two or more Member States or a single Member State if the critical infrastructure is located in another Member State. This procedure is based on a three step process. First, the Commission together with the Member States and relevant stakeholders develop cross-cutting and sectoral criteria for the identification of ECI, which are then adopted through the comitology procedure. The cross-cutting criteria are developed on the basis of severity of the disruption or destruction of the CI. The severity of the consequences of the disruption or destruction of a particular infrastructure should be assessed on the basis, where possible, of:

- Public effect (number of population affected);
- Economic effect (significance of economic loss and/or degradation of products or services);
- Environmental effect;
- Political effects;
- Psychological effects;
- Public health consequences.

Each Member State then identifies those infrastructures which satisfy the criteria. Finally, each Member State notifies the Commission of the critical infrastructures which satisfy the established criteria. Relevant work is undertaken under priority CIP sectors selected by the Commission on an annual basis from among those listed in Annex I. The list of CIP sectors contained in Annex I may be amended through the comitology procedure in so far as this does not broaden the scope of the Directive. This would in particular mean that amendments to the list would be made for the purpose of clarifying its contents. The Commission considers the transport and energy sectors as being amongst the immediate priorities for action.

Article 4 – the procedure for designating ECI is set out. Following the identification procedure completed pursuant to Article 3, the Commission prepares a draft list of ECI. The draft list is based on the notifications received from the Member States and other relevant information from the Commission. The list is then adopted through comitology.

Article 5 – Operator Security Plans (OSPs). Article 5 requires all CI owners/operators designated as ECI to establish an OSP which identify the ECI owners' and operators' assets

and establish relevant security solutions for their protection. Annex II provides the minimum contents of such OSPs including:

- 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.

Each CIP sector may develop sector-specific OSPs based on the minimum requirements of Annex II. Such sector specific OSPs may be adopted through comitology.

For those sectors in which similar obligations already exist, Article 5(2) foresees the possibility of being exempted from the OSP obligations based on a decision taken through comitology. It is acknowledged that Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security already satisfies the requirement to establish an Operator Security Plan.

Once an OSP has been created, each ECI owner/operator should submit the OSP to the relevant Member State authority. Each Member State will setup a supervisory system concerning OSPs which will ensure that sufficient feedback is given to the ECI owner/operator concerning the quality of the OSP and in particular the adequacy of the risk and threat assessment.

Article 6 – the Security Liaison Officer (SLO). Article 6 requires all CI owners/operators designated as ECI to appoint an SLO. The SLO would function as the point of contact for security issues between the ECI and the relevant CIP authorities in the Member States. The SLO would therefore receive all relevant CIP related information from the Member State authorities and would be responsible for providing relevant information from the ECI to the Member State.

Article 7 – reporting. Article 7 introduces a series of reporting measures. Each Member State is required to conduct a risk and threat assessment concerning ECI. This information shall form the basis for the MS' dialogue on security issues (supervision) with ECI as indicated in Article 5. Since Article 5 requires ECI owners/operators to establish OSPs and submit them to the MS authorities, each Member State is asked to elaborate a generic overview of the types of vulnerabilities, threats and risks encountered in each CIP sector, and to provide this information to the Commission. This information will form the basis for the Commission's

assessment whether additional protection measures may be required. The information may later be used for the development of impact assessments, which would accompany future proposals in this area.

This article also envisages the development of common methodologies for carrying out risk, threat and vulnerability assessments in respect of ECIs. Such common methodologies would be adopted through the comitology procedure.

Article 8 – Commission support for ECI. The Commission will support ECI owners/operators by providing access to available best practices and methodologies related to CIP. The Commission will undertake to collect such information from various sources (e.g. Member States, own development) and make it available to those concerned.

Article 9 – CIP Contact Points. In order to ensure cooperation and coordination of CIP issues, each Member States is required to designate a CIP Contact Point. The Contact Point would coordinate CIP issues within the Member State, with other Member States and with the Commission.

Article 10 – Confidentiality and CIP information exchange. Confidentiality and CIP information exchange is a crucial and sensitive element of work on CIP. As a consequence, the Directive requires the Commission and MS to take appropriate measures to protect information. Any personnel handling classified CIP information should have the necessary security vetting provided by the Member State authorities.

Article 11 – Committee. Certain elements of the Directive will be implemented through comitology. The Committee will be composed of the CIP Contact Points. The advisory procedure will be used for the purpose of Article 5(2) that is to exempt particular sectors from the obligation of developing an OSP.

The regulatory procedure is envisaged for the following issues:

- Article 3(1) – adoption of the cross-cutting and sector specific criteria to identify ECI
- Article 3(2) – amending the list of CIP sectors found in Annex I.
- Article 4(2) – adoption of the draft list of ECI
- Article 5(2) – development of sector specific requirements concerning OSPs
- Article 7(2) – development of a common template for generic reports concerning identified risks, threats and vulnerabilities
- Article 7(4) – development of common methodologies for carrying out risk, threat and vulnerability assessments.

2006/0276 (CNS)

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

(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,

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

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

Having regard to the opinion of the European Central Bank[3],

Whereas:

(1) In June 2004, the European Council asked for the preparation of an overall strategy to protect critical infrastructures[4]. In response, on 20 October 2004, the Commission adopted a Communication on Critical Infrastructure Protection in the Fight against Terrorism[5] 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[6] 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

---

1 OJ C […], […], p. […].
2 OJ C […], […], p. […].
3 OJ C […], […], p. […].
4 Council document 10679/2/04 REV 2.
5 COM(2004) 702.
6 COM(2005) 576.

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 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[7].

(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.

Article 2
Definitions

For the purpose of this directive:

a) “Critical Infrastructure” means those assets or parts thereof which are essential for the maintenance of critical societal functions, including the supply chain, 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 two or more Member States, or a single Member State if the critical infrastructure is located in another Member State. 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);

[7] OJ L 184, 17.7.1999, p. 23.

- economic effect (significance of economic loss and/or degradation of products or services);
- environmental effect;
- political effects;
- psychological effects
- public health consequences;

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;

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 to the asset, and the likelihood that a specific vulnerability will be exploited by a particular threat;

g) "Critical 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.

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.

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.

LEGISLATIVE FINANCIAL STATEMENT

Policy area(s): Justice and Home Affairs

Activity: Critical Infrastructure Protection

TITLE OF ACTION: Directive of the Council on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection

1. BUDGET LINE(S) + HEADING(S)

NA

2. OVERALL FIGURES

2.1. Total allocation for action (Part B): € million for commitment

NA

2.2. Period of application:

Starting 2006

2.3. Overall multiannual estimate of expenditure:

(a) Schedule of commitment appropriations/payment appropriations (financial intervention) *(see point 6.1.1)*

€ million (*to three decimal places)*

	[2006]	[2007]	[2008]	[2009]	[2010]	[2011]	Total
Commitments	-	-	-	-	-	-	-
Payments	-	-	-	-	-	-	-

(b) Technical and administrative assistance and support expenditure *(see point 6.1.2)*

Commitments	-	-	-	-	-	-	-
Payments	-	-	-	-	-	-	-

Subtotal a+b	-	-	-	-	-	-	-
Commitments	-	-	-	-	-	-	-
Payments	-	-	-	-	-	-	-

(c) Overall financial impact of human resources and other administrative expenditure *(see points 7.2 and 7.3)*

Commitments/ payments	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000

TOTAL a+b+c	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000
Commitments	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000
Payments	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000	1.280.000

2.4. Compatibility with financial programming and financial perspective

The Directive is compatible with the Programme Prevention, Preparedness and consequence Management of Terrorism and other Security related Risks, for the period 2007-2013.

2.5. Financial impact on revenue:

The recently adopted programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security and Safety Related Risks" for the period 2007-2013 (€ 137.5 million) will contribute to the implementation of EPCIP against security risks and those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the critical functions of society as part of the general programme "Security and safeguarding liberties". The programme is limited in scope as it does not cover the investments related to hardware or equipment. This programme does not apply to matters that are covered by other financial instruments and in particular the Rapid Response Instrument in the event of major emergencies.

With regard to prevention and preparedness, the programme aims at:

a) stimulating, promoting, and supporting risk and threat assessments on critical infrastructure, including evaluations on site to identify threats and vulnerabilities and needs for upgrading their security;

b) promoting and supporting common operational measures to improve security in cross-border supply chains, provided that the rules of competition within the internal market are not distorted;

c) promoting and supporting the development of minimum security standards, exchange of best practices, risk assessment tools, methodologies to compare and prioritise infrastructure in different sectors, analysis of vulnerabilities and interdependencies on protection of critical infrastructure;

d) promoting and supporting Community wide coordination and cooperation on protection of critical infrastructure. Where relevant development of proposals for minimum protection measures and common guidelines.

With regard to consequence management, the programme aims at:

a) stimulating, promoting and supporting exchange of know-how, experience and technology;

b) stimulating, promoting and supporting the development of relevant methodology and contingency plans;

c) ensuring real-time input of specific expertise on security matters within overall crisis management, rapid alert and civil protection mechanisms.

The proposal therefore has no financial implications on revenue.

3. BUDGET CHARACTERISTICS

Type of expenditure		**New**	**EFTA contribution**	**Contributions from applicant countries**	**Heading in financial perspective**
Non-comp	Non-diff	NA	NA	NA	**No** NA

4. LEGAL BASIS

The legal basis for the proposal is Article 308 of the Treaty establishing the European Community.

5. DESCRIPTION AND GROUNDS

5.1. Need for Community intervention

5.1.1. Objectives pursued

A Directive is best suited to create the common EPCIP framework as the Member States have varying approaches to critical infrastructure protection and different legal traditions. By putting forward a number of key ideas and allowing the Member States to make use of approaches best suited to their needs, the objectives of EPCIP can be fully realised while building on what has already been achieved.

5.1.2. Measures taken in connection with ex ante *evaluation*

All relevant stakeholders have been consulted concerning the development of EPCIP. This has been done through:

- The EPCIP Green Paper adopted in on 17 November 2005 with the consultation period ending on 15 January 2006. 22 Member States provided official responses to the consultation. Around 100 private sector representatives also provided comments to the Green Paper. The responses were generally supportive of the idea of creating EPCIP.

- Three Critical Infrastructure Protection seminars hosted by the Commission (in June 2005, September 2005 and March 2006). All three seminars brought together representatives of the Member States. The private sector was invited to the seminars held in September 2005 and March 2006.

- Informal meetings of CIP Contact Points. The Commission hosted two meetings of the CIP Contact Points of the Member States (December 2005 and February 2006).

- Informal meetings with private sector representatives. Numerous informal meetings were held with representatives of particular private business as well as with industry associations.

- Internally, within the Commission, work on the development of EPCIP was taken forward with the help of regular meeting of the sub-group on Critical Infrastructure Protection on the Inter-Service Group on the Internal Aspects of Terrorism.

5.2. Action envisaged and budget intervention arrangements

The budgetary impact is estimated in the accompanying financial statement.

5.3. Methods of implementation

It is a Directive hence no method of budgetary implementation necessary.

6. FINANCIAL IMPACT

6.1. Total financial impact on Part B - (over the entire programming period)

6.1.1. Financial intervention

NA

6.1.2. Technical and administrative assistance, support expenditure and IT expenditure (commitment appropriations)

NA

6.2. Calculation of costs by measure envisaged in Part B (over the entire programming period)

NA

7. IMPACT ON STAFF AND ADMINISTRATIVE EXPENDITURE

7.1. Impact on human resources

Types of post		Staff to be assigned to management of the action using existing resources		Total	Description of tasks deriving from the action
		Number of permanent posts	Number of temporary posts		
Officials or temporary staff	A B C	8 A 1 B	1 C	10	Gathering and processing of information, preparing the Committee meetings
Other human resources					
Total		9	1	10	

The needs for human and administrative resources shall be covered within the allocation granted to the managing DG in the framework of the annual allocation procedure.

7.2. Overall financial impact of human resources

Type of human resources	Amount (€)	Method of calculation *
Officials Temporary staff	1.080.000 48.000	(108.000x10=1.080.000 4.000 x 12 = 48.000
Other human resources (specify budget line)		
Total	1.128.000	

The amounts are total expenditure for twelve months.

7.3. Other administrative expenditure deriving from the action

Budget line (number and heading)	Amount €	Method of calculation
Overall allocation (Title A7)		
A0701 – Missions	24.000	2000x12 months=24.000
A07030 – Meetings	-	-
A07031 – Compulsory committees	128.000	32.000 x 4 meetings a year=128.000
A07032 – Non-compulsory committees	-	-
A07040 – Conferences	-	-
A0705 – Studies and consultations	-	-
Other expenditure (specify)		
Information systems (A-5001/A-4300)	-	-
Other expenditure - Part A (specify)		

Total	152.000	

The amounts are total expenditure for twelve months.

Specify the type of committee and the group to which it belongs.

I.	Annual total (7.2 + 7.3)	1.280.000
II.	Duration of action	Ongoing
III.	Total cost of action (I x II)	

8. FOLLOW-UP AND EVALUATION

8.1. Follow-up arrangements

NA

8.2. Arrangements and schedule for the planned evaluation

NA

9. ANTI-FRAUD MEASURES

NA