

EUROPEAN PARLIAMENT

2004



2009

Committee on Civil Liberties, Justice and Home Affairs

PROVISIONAL
2006/0276(CNS)

18.4.2007

*

DRAFT REPORT

on the proposal for a Council directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection

(COM(2006)0787 – C6-0053/2007 – 2006/0276(CNS))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Jeanine Hennis-Plasschaert,

Symbols for procedures

- * Consultation procedure
majority of the votes cast
- **I Cooperation procedure (first reading)
majority of the votes cast
- **II Cooperation procedure (second reading)
*majority of the votes cast, to approve the common position
majority of Parliament's component Members, to reject or amend
the common position*
- *** Assent procedure
*majority of Parliament's component Members except in cases
covered by Articles 105, 107, 161 and 300 of the EC Treaty and
Article 7 of the EU Treaty*
- ***I Codecision procedure (first reading)
majority of the votes cast
- ***II Codecision procedure (second reading)
*majority of the votes cast, to approve the common position
majority of Parliament's component Members, to reject or amend
the common position*
- ***III Codecision procedure (third reading)
majority of the votes cast, to approve the joint text

(The type of procedure depends on the legal basis proposed by the Commission.)

Amendments to a legislative text

In amendments by Parliament, amended text is highlighted in ***bold italics***. Highlighting in *normal italics* is an indication for the relevant departments showing parts of the legislative text for which a correction is proposed, to assist preparation of the final text (for instance, obvious errors or omissions in a given language version). These suggested corrections are subject to the agreement of the departments concerned.

CONTENTS

	Page
DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION	5
EXPLANATORY STATEMENT	19

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

on the proposal for a Council directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection

(COM(2006)0787 – C6-0053/2007 – 2006/0276(CNS))

(Consultation procedure)

The European Parliament,

- having regard to the Commission proposal to the Council (COM(2006)0787)
 - having regard to Article 308 of the EC Treaty, pursuant to which the Council consulted Parliament (C6-0053/2007),
 - having regard to the Council Conclusions of 1-2 December 2005 on the principles for a European Programme on Critical Infrastructures,
 - having regard to Rule 51 of its Rules of Procedure,
 - having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs and the opinions of the Committee on Economic and Monetary Affairs, the Committee on Industry, Research and Energy and the Committee on Transport and Tourism (A6-0000/2007),
1. Approves the Commission proposal as amended;
 2. Calls on the Commission to alter its proposal accordingly, pursuant to Article 250(2) of the EC Treaty;
 3. Calls on the Council to notify Parliament if it intends to depart from the text approved by Parliament;
 4. Calls for initiation of the conciliation procedure under the Joint Declaration of 4 March 1975 if the Council intends to depart from the text approved by Parliament;
 5. Asks the Council to consult Parliament again if it intends to amend the Commission proposal substantially;
 6. Instructs its President to forward its position to the Council and Commission.

Text proposed by the Commission

Amendments by Parliament

Amendment 1 Recital 2

(2) On 17 November 2005 the Commission

(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 (CIWIN). The responses received to the Green Paper **clearly showed the need to set up** a Community framework concerning critical infrastructure protection. The need to increase the critical infrastructure protection capability in Europe and to help reduce vulnerabilities concerning critical infrastructures was acknowledged. The importance of the **principle** of subsidiarity and of stakeholder dialogue was emphasised.

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 (CIWIN). The responses received to the Green Paper **underlined the possible 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, confidentiality and complementarity as well as** of stakeholder dialogue was emphasised.

Justification

More in line with reality.

Amendment 2

Recital 3

(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.***

(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.

Justification

Superfluous.

Amendment 3
Recital 4

(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.

(4) The primary **and ultimate** responsibility for protecting critical infrastructures falls on the Member States and the owners/operators of critical infrastructures. This should not change. ***Bearing in mind that national services know best what is happening in their countries, a bottom-up approach towards European Critical Infrastructure (ECI) should therefore be taken.***

Justification

It must be clear that the primary and ultimate responsibility falls on the MS. The Community approach should not duplicate the work of the Member States.

Amendment 4
Recital 5

(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.

(5) There are a certain number of critical infrastructures in the Community, the disruption or destruction of which would affect **three** or more Member States or **at least two** Member **States** 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 **European** 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.

Justification

An European approach is justified if at least three Member States would be affected or at least two Member States other than that in which the critical infrastructure is located.

Amendment 5

Recital 6

(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

(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 **should ensure** 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 **European** critical infrastructure protection

Justification

As most critical infrastructure is privately owned and operated, the EU approach should fully involve the private sector and be built on existing sector-based protection measures, taking into account sector characteristics.

Amendment 6

Recital 7

(7) Each owner/operator of European critical infrastructure should establish an Operator Security Plan identifying critical assets and laying down relevant security

(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.

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.

Compliance with existing sector-based protection measures could satisfy the requirement to establish and update an Operator Security Plan.

Justification

The Community approach should be built on existing sector-based protection measures, taking into account sector characteristics. Contradictions or duplications should be avoided at all costs.

Amendment 7
Recital 8

(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.

(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. ***Compliance with existing sector-based protection measures could satisfy the requirement to designate a Security Liaison Officer.***

Justification

The Community approach should be built on existing sector-based protection measures, taking into account sector characteristics. Contradictions or duplications should be avoided at all costs.

Amendment 8
Recital 11

(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

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

infrastructure protection.

concerning critical infrastructure protection.

Justification

Wording of original paragraph is too strong.

Amendment 9

Recital 12

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

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

Amendment 10

Recital 13

(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.

(13) In order to develop **European** Critical Infrastructure Protection activities in areas which require a degree of confidentiality, it is **crucial** to ensure a coherent and secure information exchange in the framework of this Directive. Certain **European** 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.

Justification

CIP information exchange is a crucial and sensitive element of work on ECIP.

Amendment 11
Recital 14

(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.***

(14) 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 data will be sufficiently protected.

Justification

Not appropriate.

Amendment 12
Recital 15

(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.

(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. ***Duplications of - or contradictions between - different acts or provisions should be avoided at all costs.***

Justification

The administrative burden should be as limited as possible.

Amendment 13
Recital 17

(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

(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.

approach to the assessment of the needs to improve the protection of such infrastructures, cannot ***in all cases*** 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.

Justification

Wording of original paragraph is too strong.

Amendment 14
Article 2, point (b)

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;

b) “European Critical Infrastructure” means critical infrastructures the disruption or destruction of which would significantly affect ***three*** or more Member States, or ***at least two Member States*** if the critical infrastructure is located in another Member State. This includes effects resulting from cross-sector dependencies on other types of infrastructure;

Justification

An European approach is justified if at least three Member States would be affected or at least two Member States other than that in which the critical infrastructure is located.

Amendment 15
Article 3, paragraph 1

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).

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

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.

in Article 11(3).

The cross-cutting criteria having a horizontal application to all **European** 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 **and be built on existing sector-based protection measures** taking into account the characteristics of individual critical infrastructure sectors, and involving **all** relevant stakeholders **as sectors possess the relevant experience, expertise and requirements concerning the protection of their critical infrastructure**. They shall be adopted for each priority sector at the latest one year following the designation as a priority sector.

Where Community mechanisms are already in place, they shall continue to be used. Duplications of - or contradictions between - different acts or provisions shall be avoided at all costs.

Justification

The Community approach should be built on existing sector-based protection measures, taking into account sector characteristics. Contradictions or duplications should be avoided at all costs.

Amendment 16

Article 3, paragraph 2, subparagraph 1

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.

2. The priority sectors to be used for the purposes of developing the criteria provided for in paragraph 1 shall be identified **in accordance with the procedure referred to in Article 11(3)** on an annual basis from among those listed in Annex I.

Justification

Extra safeguard.

Amendment 17
Article 3, paragraph 3

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.

3. Each Member State shall identify the ***possible European*** critical infrastructures located within its territory as well as ***possible European*** 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 ***possible European*** critical infrastructures thus identified at the latest one year after the adoption of the relevant criteria and thereafter on an ongoing basis.

Amendment 18
Article 4, paragraph 2, subparagraph 1

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)***.

2. The list of critical infrastructures designated as European Critical Infrastructure shall be adopted ***by the Council***.

Justification

The primary and ultimate responsibility falls on the Member States.

Amendment 19
Article 5, paragraph 1

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.

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. ***Acting in accordance with the procedure referred to in Article 11(3), a list of existing protection measures applicable to specific sectors listed in Annex I shall be adopted. Compliance with one or more of the listed protection measures satisfies the requirement to***

establish and update an Operator Security Plan.

Justification

Contradictions between - or duplications of existing measures should be avoided at all costs.

Amendment 20
Article 5, paragraph 2, subparagraph 2

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. ***deleted***

Justification

Contradictions between - or duplications of existing measures should be avoided at all costs.

Amendment 21
Article 5, paragraph 3

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.

3. The owner/operator of a European Critical Infrastructure shall submit the Operator Security Plan to ***the relevant CIP Contact Point*** 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 CIP Contact Point*** within 1 year following the adoption of the sector specific requirements.

Justification

One-stop-shop principle.

Amendment 22
Article 5, paragraph 5

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. *deleted*

Justification

By listing one, you exclude others. See the proposed addition to paragraph 1.

Amendment 23
Article 6, paragraph 1

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.

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 CIP Contact Point*** 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. ***Acting in accordance with the procedure referred to in Article 11(3), a list of existing protection measures applicable to specific sectors listed in Annex I shall be adopted. Compliance with one or more of the listed protection measures satisfies the requirement to designate a Security Liaison Officer.***

Justification

Contradictions between - or duplications of existing measures should be avoided at all costs.

Amendment 24
Article 6, paragraph 2

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

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

Justification

One-stop-shop principle. The administrative burden should be as limited as possible.

Amendment 25
Article 7, paragraph 3

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

3. **Acting in accordance with the procedure referred to in Article 11(3), an assessment on a sectoral basis will be made in order to identify** whether specific protection measures are required for European Critical Infrastructures.

Justification

Extra safeguard.

Amendment 26
Article 7, paragraph 4

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).

4. **If deemed to be necessary**, 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). **Such common methodologies shall take into account existing methodologies.**

Justification

Contradictions between - or duplications of existing measures should be avoided at all costs.

Amendment 27
Article 10, paragraph 2

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.

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

Amendment 28
Article 10, paragraph 3

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.

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

Amendment 29
Article 12, paragraph 1, subparagraph 1

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.

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by **1 July 2008** 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.

Justification

More realistic.

EXPLANATORY STATEMENT

GENERAL BACKGROUND:

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 the 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.

The legal basis for the proposal is Article 308 of the Treaty establishing the European Community. Information was collected from all relevant stakeholders.

As currently no horizontal provisions on critical infrastructure protection exist at EU level, the Commission's proposal intends to create a horizontal framework for the identification and designation of European Critical Infrastructures and for the assessment of needs to improve their protection.

Following the Commission's proposal only a common framework, by way of a directive, 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.

RAPPORTEUR'S POSITION:

The rapporteur supports the idea of a common framework. Indeed, 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. 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.

The vulnerability of critical infrastructures and the ensuing vulnerability of the services they provide, require action. And effective protection of vulnerable critical infrastructures and services requires communication, coordination and cooperation - nationally and at EU level, involving all relevant stakeholders.

Furthermore, experiences from the past do tell us that if a terrorist attack occurs, the EU Heads of State will be calling for new security proposals within forty-eight hours, thereby weakening the quality of possible proposals. Or even worse, they come up with measures that are disproportionate and lack transparency, like for example the measures restricting liquids aboard aircrafts.

The establishment of horizontal provisions at EU-level, whereby the complex processes and interfaces of critical infrastructures with a trans-national dimension are taken into account, is therefore a legitimate concern.

At the same time, however, it should be recognised that the EU should support and not duplicate the work of the Member States. A bottom-up approach should be taken, bearing in mind that national services know best what is happening in their countries.

Having said that, the rapporteur is of the opinion that a Community approach can only be justified if at least three Member States would be affected or at least two Member States other than that in which the critical infrastructure is located.

It is important for her to recall that the primary and ultimate responsibility for protecting critical infrastructures falls on the Member States and the owners/operators of critical infrastructures. And as private sector possess particular experience, expertise and requirements concerning the protection of their critical infrastructures, it is of utmost importance to fully involve the private sector.

Moreover, the rapporteur would like to stress that duplication of - or contradiction between different acts or provisions should be avoided at all costs. Possible future common assessment methodologies, if deemed to be necessary, should thus take into account existing methodologies. Cross-cutting and sectorial criteria should thus be built on existing sector-based protection measures, taking into account the characteristics of individual critical infrastructure sectors. Where Community mechanisms are already in place, they should continue to be used. And compliance with one or more of the existing protection measures, could satisfy the requirement to establish and update an Operator Security Plan and/or the requirement to designate a Security Liaison Officer.

Finally, the rapporteur believes that the administrative burden should be as limited as possible, respecting inter alia the "One-stop-shop" principle.