



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 9 November 2007

14915/07

**Interinstitutional File:
2006/0276 (CNS)**

LIMITE

**PROCIV 194
JAI 573
COTER 79
ENER 269
TRANS 350
TELECOM 136
ATO 151
ECOFIN 440
ENV 600
SAN 198
CHIMIE 37
RECH 352
DENLEG 108
RELEX 832**

**DOCUMENT PARTIALLY
ACCESSIBLE TO THE PUBLIC**

NOTE

from : the Presidency

to : the Working Party on Civil Protection

No. prev. doc. : 14083/07 PROCIV 166 JAI 515 COTER 71 ENER 247 TRANS 310
TELECOM 120 ATO 127 ECOFIN 400 ENV 530 SAN 176 CHIMIE 30
RECH 264 DENLEG 95 RELEX 740

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

Subject : Proposal for a Directive of the Council on the identification and designation of
European Critical Infrastructure and the assessment of the need to improve their
protection

I. INTRODUCTION

1. The Working Party on Civil Protection examined, with the participation of critical infrastructure protection experts, at its meeting on 30 October 2007 Annex 1 of the above-mentioned Commission proposal. Based on these discussions, the Presidency submits this note.
2. In order to take work on this file forward, the Presidency also encourages delegations to send any comments or text proposals they may have to the Presidency (DELETED) and a copy to the Council Secretariat (DELETED).

II. STATE OF PLAY IN THE NEGOTIATIONS ON THE PROPOSED DIRECTIVE

3. The Commission submitted to the Council and Parliament, on 18 December 2006, the above proposal.
4. The European Central Bank issued its opinion on 13 April 2007 (8987/07). The Working Party on Civil Protection examined the opinion at its meeting on 27 June 2007.
5. The European Parliament issued its opinion on 10 July 2007 (the provisional version of the opinion is contained in doc. P6_TA-PROV (2007)0325). The Working Party on Civil Protection examined the opinion at its meetings on 26 July and 13 September 2007.
6. Several delegations announced that they would enter general parliamentary scrutiny reservations.
7. Following the discussions of the Working Party on Civil Protection on Articles 1 to 14 of the proposed Directive, in particular the following questions remain outstanding:
 - DE, supported by DK/SE, entered an overall reservation on the approach proposed by Cion and, as one possible alternative, proposed the adoption of a *Council*

Decision establishing a mechanism for the exchange of information and best practices as well as for the preparation of recommendations regarding European Critical Infrastructure priority sectors in order to improve their protection (14282/07). Therefore, all detailed comments made by DE/DK/SE on the proposed Directive are to be seen in the light of this overall rejection of the approach proposed by the Commission. CZ/MT/UK noted that some elements of the approach proposed by DE deserved further consideration. Therefore, DE is of the view that an in-depth discussion of its approach is needed. The approach suggested by DE has been presented at the meetings of the Working Party on 14 September and 9 October 2007; it has been discussed on 9 October 2007.

- UK entered a reservation against the inclusion of hazardous infrastructures in Article 2 (a) (2); the hazardous sectors (nuclear, chemical and dams) should be excluded from the scope of the ECI designation process. DE entered a reservation against the inclusion of nuclear issues in Article 2 (a) (2) and the use of Article 203 of the *Treaty establishing the European Atomic Energy Community* as a legal basis. NL/SE entered a scrutiny reservation on Article 2 (a) (2).
- DE/DK/EE/NL/UK/SE requested that, in order to meet the definition of "European Critical Infrastructures" in Article 2 (b), the disruption or destruction of the critical infrastructure should have a significant impact on at least three (instead of "two") Member States. DE/IE/NL entered a reservation on the compromise proposal proposed by the Presidency (see Annex; same wording as in 14083/07); UK asked for further explanations of the Presidency proposal; PL explicitly stated that it was in favour of the text as it had been proposed by Cion.

- Following comments made by several delegations that the cross-cutting as well as at least some of the sector specific criteria (Article 3 (1)) have to be adopted at the same time as the directive itself, Cion made a presentation on cross-cutting criteria at the meeting on 30 October 2007; moreover, Cion accepted that it would submit proposals on some sector-specific criteria before the meeting on 20 November 2007. These criteria would be annexed to the proposed Directive. The priority sectors to be considered at this stage will be transport and energy as well as information and communication technologies.

- DE entered a reservation against the necessity of definitions in Article 2 (c) to (g).

- Following discussions on the proposed lists of critical infrastructures, a new version of Articles 3 (3) and 4 was submitted to delegations (see Annex; same wording as in 14083/07). CZ/ DE/PL entered a reservation against this new version; SI requested clarification on the new version and in particular raised the concern that the procedure described in these articles might lead to a duplication of work.

- DE/CZ/SE entered a reservation against an obligation to establish Operator Security Plans (OSPs, Article 5), inter alia because their implementation would entail that ECIs could be identified by the public. UK also opposed obligatory OSPs as there had been no need identified for them to be legally required. NL/SK would oppose an obligation if the minimum requirements for the OPS were too detailed. In response to certain concerns by those Member States which already oblige their critical infrastructure owners/operators to implement OSPs, a compromise proposal was submitted by Cion before the last meeting (see Annex; same wording as in 14083/07) in order to reflect that if security plans or their equivalents are already in place, there would be no further need to legislate or introduce new obligations on owners/operators. This compromise proposal has not yet been discussed.

- DK/SE/UK expressed their opposition to the obligation of owners/operators of ECI to designate Security Liaison Officers as proposed in Article 6; DE entered a reservation. A compromise proposal submitted by Cion before the last meeting (14083/07) has not yet been discussed.

- With respect to the protection of sensitive CIP-related information, SE entered a reservation against Article 9 (1), second sub-para.

- NL did not see a role for a committee and therefore suggested deleting Article 11; DE requested deleting this Article.

- AT submitted a non-paper on Article 12 (14306/07) which will be presented and discussed at the next meeting; DE entered a reservation on Article 12. A new proposal from Cion is contained in the Annex.

- Comments made on the Annexes to the proposed directive are reflected in footnotes.

DRAFT

DIRECTIVE OF THE COUNCIL

**on the identification and designation of European Critical Infrastructure and the
assessment of the need to improve their protection¹**

(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,]²

Having regard to the proposal from the Commission³,

Having regard to the opinion of the European Parliament⁴,

Having regard to the opinion of the European Central Bank⁵,

¹ **DE**, supported by **DK/SE**, entered an overall reservation against the proposed directive and instead suggested adopting a *Council Decision establishing a mechanism for the exchange of information and best practices as well as for the preparation of recommendations regarding European Critical Infrastructure priority sectors in order to improve their protection*. Parliamentary scrutiny reservation by **DE/DK/SE/UK**. General scrutiny reservation by **RO**.

² Reservation by **DE** regarding the use of Article 203 of the *Treaty establishing the European Atomic Energy Community* as a legal basis. **FR** requested the inclusion of the following paragraph into the text of the proposed directive: "*The present directive does not create any new competence of the Community with regard to security and concerning nuclear infrastructures, any common measures that could be decided should be based on the Euratom treaty.*"

³ OJ C [...], [...], p. [...].

⁴ OJ C [...], [...], p. [...].

⁵ OJ C 116, 26.5.2007, p. 1.

Whereas⁶:

- (1) In June 2004, the European Council asked for the preparation of an overall strategy to protect critical infrastructures⁷. In response, on 20 October 2004, the Commission adopted a Communication on Critical Infrastructure Protection in the Fight against Terrorism⁸ 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 Protection⁹ 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.

⁶ **The recitals will be examined following agreement on the articles.**

⁷ 10679/2/04 REV 2.

⁸ 13979/04

⁹ 14910/05

- (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 protection¹⁰¹¹.

¹⁰ **Cion** suggested inserting an additional recital (6a): *"For the purposes of the financial sector, this Directive should be compatible with the tasks and duties conferred on the European System of Central Banks (ESCB) by the Treaty and the Statute of the European System of Central Banks and of the European Central Bank, and on National Central banks, Financial Regulatory Authorities and Financial Supervisory Authorities under other equivalent EU or national provisions. Particular attention in this regard needs to be given to the operation and oversight of payment and securities trading, clearing and settlement infrastructures and systems by the ESCB central banks, and to the contribution made by central banks to the stability of the financial system. To avoid unnecessary duplication of work, Member States should rely on the work and regular assessments conducted by National Central Banks, the European central bank and Financial Regulatory and Supervisory Authorities within their fields of competence."*

¹¹ **Cion** suggested inserting an additional recital (6b): *"To avoid duplication with existing requirements adopted by Member States for the protection of nuclear facilities and nuclear material against acts which could directly or indirectly endanger the health and safety of the public or the environment by exposure to radiation or release of radioactive substances, implementation of this Directive shall fully recognise the provisions of Article 2A of the Convention on the Physical Protection of Nuclear Material (as amended by the Amendment adopted at Vienna on 8th July 2005). Following the entry into force of the amended Convention, the implementation of the provisions of this Article shall be deemed to satisfy the requirements of this Directive in respect of the protection of the nuclear industry (including nuclear power stations) against such acts."*

- (7) Each owner/operator of European Critical Infrastructure should establish an Operator Security Plan identifying critical assets and laying¹² 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.¹³¹⁴
- (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.

¹² **Cion** suggested replacing the first part of this sentence by: *"An Operator Security Plan should be established for each European critical infrastructure. It should identify critical assets and lay (down...)."*

¹³ **Cion** suggested replacing this sentence by: *"The Operator Security Plan should include a risk analysis and take into account other relevant information provided by Member States. Pursuant to article 249 of the Treaty establishing the European Community, it is up to each Member State to select the appropriate form and methods in order to achieve the requirement of having an Operator Security Plan for each European Critical Infrastructure as set out in this Directive. Sectors, including the financial sector, in which there are already in place measures, principles, guidelines including Community measures that refer to the need to have a plan similar or equivalent to an Operator Security Plan and where compliance with relevant measures, principles or guidelines is ensured, will be deemed to satisfy the requirements in relation to an Operator Security Plan."*

¹⁴ **UK** suggested inserting an additional recital 6 (c): *"The relevant Member State authorities that will be involved in the ECI process will be defined by the Member State, taking into account the variations for different sectors."*

- (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 access¹⁵ to best practices and methodologies concerning critical infrastructure protection.

¹⁵ **UK** suggested inserting "*through relevant Member State authorities*".

(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 coordinate¹⁶ CIP issues internally, as well as with other Member States and the Commission.

¹⁶ **UK** suggested inserting "*European*".

- (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 Protection¹⁷ information is of such nature that its disclosure would undermine the protection of the public interest as regards public security¹⁸. Specific facts about a critical infrastructure asset, which could be used to plan and act with a view to causing unacceptable consequences¹⁹ 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.²⁰²¹²²

¹⁷ **Cion** suggested replacing “*Certain Critical Infrastructure Protection (information...)*” by “*Sensitive Critical Infrastructure Protection related (information...)*”.

¹⁸ **UK** suggested replacing “*public interest as regards public security*” by “*infrastructure*”.

¹⁹ **UK** suggested replacing “*unacceptable consequences*” by “*disruption or destruction*”.

²⁰ **Cion** suggested adding the following sentence: “*Each Member State should respect the relevant security classification of sensitive documents given by the originator of the document*”.

²¹ **SE** suggested replacing the second sentence of this para. by: “*It is important that the rules of confidentiality according to applicable national law or the Regulation (EC) No. 1049/2001 regarding public access to European Parliament, Council and Commission documents are observed with regard to specific facts about critical infrastructure asset, which could be used to plan and act with a view to causing unacceptable consequences for critical infrastructure installations. Classified information should be protected in accordance with relevant Community legislation.*”

²² **Cion** suggested adding the following new recital: “*Without prejudice to the right of public access to European Parliament, Council and Commission documents according to Regulation (EC) no. 1049/2001 of the European Parliament and of the Council, 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. Each Member State and the Commission shall respect the relevant security classification given by the originator of a document.*”

- (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 encouraged²³.
- (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.²⁴

²³ **Cion** suggested inserting two additional recitals: "*(14a) Generic data pursuant to summary reports concerning vulnerabilities, threats and risks submitted to the Commission by the Member State will be classified at an appropriate level. Similarly, the lists of European Critical Infrastructure shall be classified at an appropriate level and access granted strictly on a need-to-know basis to relevant Commission and Member State officials having the necessary security vetting. The reports submitted to the Commission should be of such a nature so as not to allow for the identification of a specific European Critical Infrastructure.*

(14 b) Relevant CIP provisions in the individual EU Member States may vary. For this reason, it is important for critical infrastructure in Europe to be identified and designated according to a common procedure. In doing this, and in order to develop CIP activities, a high degree of confidentiality also within Member States is a precondition. The security procedures for access to CIP documents on the national level shall be established according to the national legislation and rules covering the handling on sensitive data."

²⁴ **Cion** suggested having this recital back-to-back with recital 6 (a) and adding the following sentence: "*Duplication of, or contradiction between, different acts or provisions shall be avoided at all cost."*

- (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^{25 26}.
- (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 objectives²⁷.

²⁵ OJ L 184, 17.7.1999, p. 23.

²⁶ **Cion** suggested inserting the following sentence: *"The comitology procedure shall only be used for the development of implementation pursuant to this Directive with a view to guaranteeing the expediency of decision making while taking into account the sensitive nature of the critical infrastructure protection process. The use of implementation measures shall not go beyond the mandate and scope set out by this Directive. The regulatory procedure shall be used for the purpose of this Directive".*

²⁷ The **European Central Bank** suggested in its opinion (OJ C 116, 26.5.2007, p. 1.) the inclusion of an additional recital (17 a): *"For the purposes of the financial sector, this Directive should be compatible with the tasks and duties conferred on the European System of Central Banks (ESCB) by the Treaty and the Statute of the European System of Central Banks and of the European Central Bank. Particular attention in this regard needs to be given to the operation and oversight of payment and securities clearing and settlement infrastructures and systems by the ESCB central banks, and to the contribution made by central banks to the stability of the financial system. To avoid unnecessary duplication of work, Member States should rely on the work and regular assessments conducted by the central banks within their fields of competence."*

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

HAS ADOPTED THIS DIRECTIVE:

Article 1

Subject-matter

This directive establishes a procedure for the identification and designation of European Critical Infrastructures, and a common approach to the assessment of the needs to improve the protection of such infrastructures in order to contribute to the protection of people.

Article 2
Definitions

For the purpose of this directive:

- a) “Critical Infrastructure” means
1. those assets, systems or parts thereof located in the EU Member States which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions; or
 2. those hazardous assets, systems or parts thereof located in the EU Member States the disruption or destruction of which would, as a direct consequence, have a significant impact in a Member State regardless of any impact due to the loss of service from that infrastructure.
- b) “European Critical Infrastructure” means critical infrastructure located in the EU Member States that fulfils sectoral and cross-cutting criteria designated as such under this Directive and the disruption or destruction of which would have a significant impact on, depending on the sector concerned, two or more Member States.. This includes effects resulting from cross-sector dependencies on other types of infrastructure;
- c) "risk analysis" means consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure.
- d) "Sensitive Critical Infrastructure Protection related Information” means facts about a critical infrastructure, which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations.

- e) "priority sectors" means those critical infrastructure protection sectors designated as such under this Directive.
- f) "protection" means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructure in order to deter, mitigate and neutralise a threat, risk or vulnerability.
- g) "ECI owners/operators" means those entities responsible for day-to-day operation and investment in a particular asset, system or part thereof designated as a European Critical Infrastructure under this Directive.

Article 3

Identification of European Critical Infrastructure

1. The cross-cutting and sectoral criteria to be used to identify European Critical Infrastructure shall be annexed to this Directive. They shall be the subject of a separate proposal made by the Commission to amend this Directive. The annex shall be classified at EU CONFIDENTIAL level.

The cross-cutting criteria having a horizontal application to all European Critical Infrastructure sectors shall be developed taking into account the severity of the impact of the disruption or destruction of a particular infrastructure. The severity of the impact shall be determined with reference to one or several of the following subject matters:

- Potential to cause casualties and public health consequences
- economic effect (significance of economic loss and/or degradation of products or services);
- public effect (number of members of the population affected including the effects on public confidence);
- environmental effect (with the exception of pollution);

For infrastructure providing a vital service in the priority sectors the cross-cutting criteria shall also take into account the availability of alternatives and the duration of disruption/time for recovery of service.

The sectoral criteria shall be developed for priority sectors taking into account the characteristics of individual European Critical Infrastructure sectors and involving relevant stakeholders through Member States and the Commission.

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(2) 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(2) in so far as this does not broaden the scope of this Directive.

3. Within 6 months of the adoption of the cross-cutting and sectoral criteria pursuant to paragraph 1, each Member State shall identify the potential European Critical Infrastructure located within its territory as well as the potential European Critical Infrastructure outside its territory that may have an impact on it, which both satisfy the criteria adopted pursuant to paragraph 1 and meet the definitions set out in Article 2(a) and 2(b), following the procedure provided in Annex III.

The Commission may identify potential European Critical Infrastructure which both satisfy the criteria adopted pursuant to paragraph 1 and meet the definitions set out in Article 2(a) and 2(b). The Commission shall forthwith notify the Member State on whose territory the potential European Critical Infrastructure is located as well as the affected Member States.

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

Article 4

Designation of European Critical Infrastructure

1. Within 9 months of the adoption of the cross-cutting and sectoral criteria pursuant to Article 3, each Member State shall inform the other Member States which may be affected by a potential European Critical Infrastructure about its identity and the reasons for classifying it as a potential European Critical Infrastructure.
2. Each Member State on whose territory a potential ECI is located shall engage in bilateral and/or multilateral discussions with the other Member States which may be affected by the potential ECI. The Commission may participate in these discussions but will not have having access to detailed information which would allow for the unequivocal identification of a particular infrastructure.

The bilateral and/or multilateral discussions shall focus on the applicability of the sectoral and cross-cutting criteria in relation to a particular potential ECI.

3. The Member State on whose territory a potential ECI is located shall designate it as a European Critical Infrastructure following an agreement between that Member State and the affected Member States. The acceptance of the Member State on whose territory the critical infrastructures to be designated as a European Critical Infrastructure is located, shall be required.
4. Within 12 months following the adoption of the cross-cutting and sectoral criteria pursuant to Article 3 and thereafter on an annual basis, the Member State on whose territory a designated ECI is located shall inform the Commission of the number of designated European Critical Infrastructure per sector and of the number of Member States dependent on each designated European Critical Infrastructure. Only those Member States affected by an ECI shall know its identity.

Article 5
Operator Security Plans

1. If a Member State satisfies itself that a designated European Critical Infrastructure does not have an Operator Security Plan addressing the issues identified in Annex II, it shall ensure that either by laws or regulations or by measures, principles or guidelines the owners/operators of ECI located on its territory prepare Operator Security Plans in line with Annex II and that these Operator Security Plans are reviewed regularly by the owners/operators of designated ECI.
2. The Operator Security Plan shall identify the assets of the European Critical Infrastructure and establish that relevant security solutions have been considered for their protection. In accordance with the procedure referred to in Article 11(2), the Operator Security Plan template contained in Annex II may be adapted to sectoral characteristics, while taking into account existing Community measures, but without broadening the scope of this Directive.
3. Each Member State shall verify that owner/operators of ECI located on its territory have developed an Operator Security Plan within one year following designation of the critical infrastructure as a European Critical Infrastructure. This period may be extended in exceptional circumstances, by agreement with the Member State authority and with a notification to the Commission.

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

4. Compliance with measures, principles or guidelines including Community measures which in a particular sector require, or refer to a need to have, a plan similar or equivalent to an Operator Security Plan and oversight by the relevant authority of such a plan, is deemed to satisfy all the requirements of Member States in, or adopted pursuant to, this Article.

Annex IV includes a non-exhaustive list of measures, principles and guidelines applicable in some sectors which are deemed to satisfy the Operator Security Plan requirements of this Directive.

Annex IV may be amended in accordance with the procedure referred to in Article 11(2).

Article 6

Security Liaison Officers

1. If a Member State satisfies itself that a designated European Critical Infrastructure does not have a Security Liaison Officer, it shall ensure that either by laws or regulations or by measures, principles or guidelines the owners/operators of ECI located on its territory designate a Security Liaison Officer. The Security Liaison officer shall function as the point of contact for security related issues between the owner/operator of the European Critical Infrastructure and the relevant Member State authority.
2. Each Member State shall implement an appropriate communication mechanism between the relevant Member State authority and the Security Liaison Officer with the objective of exchanging relevant information concerning identified risks and threats in relation to the European Critical Infrastructure concerned. This communication mechanism shall be without prejudice to national requirements concerning access to sensitive and classified information.

Article 7
Reporting

1. Each Member State shall conduct relevant risk analyses 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 every 24 months to the Commission generic data on a summary basis on the types of vulnerabilities, threats and risks encountered per ECI sector referred to in Annex I in which ECI is located on its territory.

A common template for these reports shall be developed in accordance with the procedure referred to in Article 11(2).

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

3. Based on the report referred to in paragraph 2, the Commission and the Member States shall assess on a sectoral basis whether further protection measures should be considered for European Critical Infrastructures.
4. Common methodological guidelines for carrying out risk analyses in respect of European Critical Infrastructures may be developed on a sectoral basis in accordance with the procedure referred to in Article 11(2). Adoption of such guidelines will be optional for the Member States.

Article 8
Commission support for ECI

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

Article 9

Sensitive CIP-related Information

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

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

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

Article 10

European CIP Contact Points

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

Article 11

Committee

1. The Commission shall be assisted by a Committee composed of the representatives of the Member States.

2. Where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall apply.

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

Article 12

Implementation

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

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

Article 13

Entry into force

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

Article 14

Addressees

This Directive is addressed to all Member States.

Done at Brussels,

For the Council

LIST OF CRITICAL INFRASTRUCTURE SECTORS²⁸

Sector	Sub-sector
I Energy	1 Oil and gas production, refining, treatment, storage and distribution by pipelines 2 All methods of electricity generation and transmission including oil, gas, solar, wind, water and nuclear power, but only in respect of supply of electricity ²⁹
II Nuclear fuel-cycle industry (for radiological hazard) ³⁰	3 Production and storage/processing of nuclear fuel-cycle substances, including within nuclear power stations

²⁸ **DE/UK** entered a reservation on the entire Annex I. **UK/NE** suggested making a distinction between sectors covering services on the one hand and, on the other hand, activities that are by their nature hazardous; **AT/DK/EE/FI/FR/PL** expressed their opposition to this suggestion.

²⁹ Reservation by **DE** against the inclusion of the gas sector and request for clarification that nuclear power plants are not included in this paragraph.

³⁰ **DE** reiterated its scrutiny reservation regarding the use of article 203 of the *Treaty establishing the European Atomic Energy Community* as a legal basis and requested the deletion of the entire sector II; reservation on sector II by **UK**; scrutiny reservation by **BE**. **Cion** argued that security matters were not addressed by this treaty which covered only safety aspects; following a request from **DK**, **Cion** agreed with including a reference to the *Convention on the Physical Protection of Nuclear Material and Nuclear Facilities* (as amended in 2005) into **Annex IV**.

III	Information, Communication Technologies, ICT ³¹	4	European Information systems ³²		
		5	Instrumentation automation and control systems (SCADA etc.) ³³		
		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	Drinking water ³⁴
				13	Control of water quality
				14	Stemming and control of water quantity
V	Food ³⁵	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		

³¹ **DE** requested the deletion of Sector III; following comments made by delegations, **Cion** suggested that, due to the horizontal nature of the ICT sectors, information systems and SCADA systems should be addressed, where relevant, within all critical infrastructure sectors in which dependence on these systems exists.

³² **UK** felt that this was not a sub-sector in its own right as it played a role also for other sectors. Scrutiny reservation by **EE/FR** against the deletion of the sub-sector 4; **IT** opposed to the deletion of this sub-sector.

³³ **UK** felt that this was not a sub-sector in its own right as it played a role also for other sectors. Consequently, **Cion** suggested the deletion of this sub-sector. **IT** opposed to the deletion; **FR** entered a scrutiny reservation.

³⁴ Reservation by **BG**.

³⁵ **DE** requested the deletion of Sector V.

VII	Financial	19	Trading, payment clearing and settlement infrastructures and systems for financial instruments ³⁶
VIII	Transport	20	Road transport ³⁷
		21	Rail transport ³⁸
		22	Air transport
		23	Inland waterways transport ³⁹
		24	Ocean and short-sea shipping

³⁶ Scrutiny reservation by DE as the banking sector was not included.

³⁷ Deletion requested by DE.

³⁸ Deletion requested by DE.

³⁹ Deletion requested by DE.

IX	Chemical industry	25	Production and storage/processing of chemical substances
		26	Pipelines of dangerous substances
X	Space	27	Space
XI	Research facilities	28	Research facilities ⁴⁰

THE IDENTIFICATION BY THE MEMBER STATES OF CRITICAL INFRASTRUCTURE WHICH MAY BE DESIGNATED AS EUROPEAN CRITICAL INFRASTRUCTURE IS DONE PURSUANT TO ARTICLE 3(3). THEREFORE THE LIST OF INFRASTRUCTURE SECTORS IN ITSELF DOES NOT GENERATE A GENERIC OBLIGATION TO DESIGNATE A EUROPEAN CRITICAL INFRASTRUCTURE IN EACH SECTOR.⁴¹

⁴⁰ **UK/Cion suggested the wording "*Scientific research facilities*"; FI/NL preferred the current wording.**

⁴¹ **DE entered a reservation against the reference to Article 3 (3) of the proposed directive.**

OPERATOR SECURITY PLAN (OSP)⁴²

The OSP shall identify the critical infrastructure owners' and operators' assets and establish relevant security solutions for their protection⁴³. The OSP will cover at least⁴⁴:

- identification of important assets;
- a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact shall be conducted;⁴⁵

⁴² **Cion** suggested to add the word "*(OSP) Procedure*".

⁴³ **Cion** suggested replacing the words "*and establish relevant security solutions for their protection*" by "*and which security solutions exist or are being implemented for their protection*".

⁴⁴ **DE/NL/SE/UK** requested the inclusion of the word "*procedure*" after "*OSP*" and expressed their opposition to a proscriptive approach. **Cion** agreed adding the word "*procedure*".

⁴⁵ **Cion** suggested to add the following definition: "*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."

- 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.⁴⁶
This heading will⁴⁷ include information concerning general measures;⁴⁸ 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 are⁴⁹ activated according to varying risk and threat levels.

⁴⁶ Following a proposal made by DK, Cion suggested to replace "*(which) cannot ... at short notice.*" by "*(which) are relevant to be employed at all times.*"

⁴⁷ DK suggested to replace "*will*" by "*may*".

⁴⁸ Cion suggested to include "*such as (technical)*".

⁴⁹ Cion suggested replacing the word "*are*" by "*can be*".

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

Article 3(3) of this Directive requires each Member State to apply the criteria adopted pursuant to Article 3(1) in order to identify those critical infrastructures which may be designated as European Critical Infrastructure. This procedure shall be implemented by each Member State through the following series of consecutive steps.

Potential European Critical Infrastructure which does not satisfy the requirements of one of the following sequential steps is considered to be ‘non-ECI’ and is excluded from the procedure. Potential European Critical Infrastructure which does satisfy the definitions shall be subjected to the next steps of this procedure.

Step 1

Each Member State shall apply the sectoral criteria adopted pursuant to Article 3(1) of this Directive in order to make a first selection of critical infrastructures within a sector.

Step 2

Each Member State shall apply the definition of critical infrastructure pursuant to Article 2(a) to the potential European Critical Infrastructure identified under step 1.

Step 3

Each Member State shall apply the definition of European Critical Infrastructure pursuant to Article 2(b) to the potential European Critical Infrastructure that has passed the first two steps of this procedure. Potential European Critical Infrastructure which does satisfy the definition will follow the next step of the procedure.

⁵⁰ **Based on a proposal by FR/IT/NL/SE/UK, Cion suggested the inclusion of Annex III.**

Step 4

Each Member State shall apply the cross-cutting criteria adopted pursuant to Article 3(1) of this Directive to the remaining potential ECI. The cross-cutting criteria shall take into account: the severity of impact; and, for infrastructure providing an essential service, the availability of alternatives; and the duration of disruption/recovery. Potential European Critical Infrastructure which does not satisfy the cross-cutting criteria will not be considered to be European Critical Infrastructure.

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

The measures, principles or guidelines referred to in Article 5(5) include:

- Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security;
- Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments (MiFID);
- Commission Directive 2006/73/EC of 10 August 2006 implementing MFID;
- Convention on the Physical Protection of Nuclear Material and Nuclear Facilities (as amended by the Amendment adopted at Vienna on 8 July 2005)⁵²;

The possibility of including the following measures is currently under consideration.

- CPSS - Core Principle VII of the Core Principles for Systemically Important Payment Systems;
- CPSS-IOSCO recommendations for Securities Settlement Systems (recommendation 11);
- CPSS-IOSCO recommendations for Central Clearing Providers (recommendation 8);

⁵¹ **Cion suggested the inclusion of Annex IV.**

⁵² **Inclusion following a request from DK/UK; PL questioned whether this convention covered also the risks arising from terrorist attacks.**