COUNCIL OF THE EUROPEAN UNION

Brussels, 21 December 2007

14915/3/07 REV 3

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**

Interinstitutional File: 2006/0276 (CNS)

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 10 December 2007 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 Council Secretariat (*secretariat.civil-protection@consilium.europa.eu*).

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 the proposed Directive, in particular the following questions remain outstanding:

- While recognising the added-value of EU-cooperation on Critical Infrastructure Protection, DE, followed by SE, requested clarification of the relationship between existing sector-specific instruments and the proposed Directive and have entered an overall reservation on the proposed Directive. DE has submitted suggestions for modifications to the Commission's proposal (14282/07). CZ has also entered an overall reservation but does not see these suggestions as the only possible alternative. DK/MT/SE/UK have noted that some elements of the approach proposed by DE deserve 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 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 and 4 was discussed at the meeting on 10 December 2007. Based on suggestions by BE, DK, LU, LV, NL, PL, UK and Cion, a compromise proposal (changes to 14915/2/07 are in bold and strikeout) is presented in this document. This compromise proposal as not yet been discussed.

- 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 and underlined the need to move away from the mandatory elements towards more encouragement. 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 implements OSPs, a new version of article 5 was discussed at the meeting on 10 December 2007. Based on suggestions by NL, UK and Cion, a compromise proposal submitted by the Presidency (changes to 14915/2/07 are in bold and strikeout) is presented in this document. This compromise proposal as not yet been discussed.

- 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.

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

- DE entered a reservation on Article 12 as it saw, based on its suggestions, no need for a provision on the implementation.

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

_____

ANNEX

DRAFT

DIRECTIVE OF THE COUNCIL

on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection[1]

(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 Commission[3],

Having regard to the opinion of the European Parliament[4],

Having regard to the opinion of the European Central Bank[5],

---

1 **DE, supported by 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.**

2 **Reservation by DE regarding the use of Article 203 of the *Treaty establishing the European Atomic Energy Community* as a legal basis**.
FR suggested a joint statement which is closely linked to FR suggestion on recital (4); a draft statement will be circulated at a later stage.

3 OJ C […], […], p. […].

4 OJ C […], […], p. […].

5 OJ C 116, 26.5.2007, p. 1.

Whereas[6]:

(1) In June 2004, the European Council asked for the preparation of an overall strategy to protect critical infrastructures[7]. In response, on 20 October 2004, the Commission adopted a Communication on Critical Infrastructure Protection in the Fight against Terrorism[8] 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[9] 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.

(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.

---

6 **The recitals will be examined following agreement on the articles.**
7 10679/2/04 REV 2.
8 13979/04
9 14910/05

(4) The primary responsibility for protecting critical infrastructures currently falls on the Member States and the owners/operators of critical infrastructures[10]. 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.

[10] **FR, supported by Cion, suggested replacing the first sentence of recital 4 by (this suggestion is linked to the joint statement suggested by FR): "*This Directive does not modify the existing powers of the EC and Euratom Communities as regards the protection of European Critical Infrastructures, the responsibility therefor falling in the first and ultimate instance on the Member States and the owners/operators of such infrastructures*".**

(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[11] [12].

---

[11] **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.".***

[12] **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 laying[13] 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.[14] [15]

(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.

---

[13] **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…).".***

[14] **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.".***

[15] **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.".***

(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[16] 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[17] CIP issues internally, as well as with other Member States and the Commission.

---

[16] **UK suggested inserting *"through relevant Member State authorities". Cion suggests: "primarily through relevant Member State authorities".***

[17] **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[18]. Certain Critical Infrastructure Protection information is of such nature that its disclosure would undermine the protection of the public interest as regards public security[19]. Specific facts about a critical infrastructure asset, which could be used to plan and act with a view to causing unacceptable consequences[20] 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.[21]

---

[18] **SE, with Cion support, suggested replacing the remaining text of the recital 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. Each Member State and the Commission should respect the relevant security classification given by the originator of a document*".**

[19] **UK suggested replacing "*public interest as regards public security*" by *"infrastructure".***

[20] **UK suggested replacing *"unacceptable consequences"* by *"disruption or destruction".***

[21] **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[22].[23]

(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[24].

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

---

22 OJ L 184, 17.7.1999, p. 23.

23 **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".***

24 **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.".***

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 the disruption or destruction of which would have a significant impact on 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) "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 **significantly** 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~~ **it provides further clarification of the sectors, but** does not broaden the scope of this Directive.

3. Within ~~6~~ **12** 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 a **significant** 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 **assist Member States to** 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~~ **15** 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 **significantly** affected by a potential European Critical Infrastructure about its identity and the reasons for ~~classifying~~ **designating** 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 **significantly** affected by the potential ECI. The Commission ~~may~~ **has the right to** 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.

   A Member State that has reason to believe that it may be significantly affected by the potential ECI, but has not been identified as such by the Member State on whose territory the potential ECI is located, may inform the Commission about its wish to be engaged in bilateral and/or multilateral discussions on this issue. The Commission shall forthwith communicate this wish to the Member State on whose territory the potential ECI is located and shall convene a meeting with the interested Member States in order to review the designation process of the 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 **significantly** 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~~ **21** 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 **significantly** 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 **accomplish** ~~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 **satisfy itself** ~~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 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

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

ANNEX I

LIST OF CRITICAL INFRASTRUCTURE SECTORS[25]

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[26]
II	Nuclear fuel-cycle industry (for radiological hazard)[27]	3	Production and storage/processing of nuclear fuel-cycle substances, including within nuclear power stations
III	Information, Communication Technologies, ICT[28]	4	European Information systems[29]
		5	Instrumentation automation and control systems (SCADA etc.)[30]
		6	Internet
		7	Provision of fixed telecommunications
		8	Provision of mobile telecommunications
		9	Radio communication and navigation
		10	Satellite communication
		11	Broadcasting

25 **DE/UK entered a reservation on the entire Annex I. UK/NL 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/EE/FI/FR/PL expressed their opposition to this suggestion.**

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

27 **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.**

28 **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.**

29 **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.**

30 **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.**

IV	Water	12	Drinking water
		13	Control of water quality
		14	Stemming and control of water quantity
V	Food[31]	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	Trading, payment clearing and settlement infrastructures and systems for financial instruments[32]
VIII	Transport	20	Road transport[33]
		21	Rail transport[34]
		22	Air transport
		23	Inland waterways transport[35]
		24	Ocean and short-sea shipping
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[36]

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.[37]

---

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

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

33 **Deletion requested by DE.**

34 **Deletion requested by DE.**

35 **Deletion requested by DE.**

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

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

ANNEX II

OPERATOR SECURITY PLAN (OSP) PROCEDURE

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

- identification of important assets;

- a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact shall be conducted;[38]

- identification, selection and prioritisation of counter-measures and procedures with a distinction between:

  - **permanent security measures**, which identify indispensable security investments and means which are relevant to be employed at all times. This heading will include information concerning general measures such as technical measures (including installation of detection, access control, protection and prevention means); organizational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems,

  - **graduated security measures**, which can be activated according to varying risk and threat levels.

_____

[38] **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.".***

ANNEX III[39]

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.

[39] **All delegations agreed in principle on the inclusion of Annex III. NL suggested that the cross-cutting criteria be applied at an earlier stage in the process. NL undertook to come up with an alternative suggestion.**

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 **significantly** affected by the potential European Critical Infrastructure.

_____

ANNEX IV

The non-exhaustive list of measures, principles or guidelines referred to in Article 5(4) 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)[40];
- Regulation 2002/2320/EC of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security[41];
- 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);

---

[40] **PL questioned whether this convention covered also the risks arising from terrorist attacks.**

[41] **Inclusion following a request from NL.**