Procedure file

Basic information

CNS - Consultation procedure Directive	2006/0276(CNS)	Procedure completed
Identification and designation of European critical infrastructures and assessment of the need to improve their protection Subject 7.30.09 Public security 7.30.20 Action to combat terrorism		

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
LIBE Civil Liberties, Justice and Home Affairs	ALDE HENNIS-PLASSCHAERT Jeanine	25/01/2007

Committee for opinion	Rapporteur for opinion	Appointed
ECON Economic and Monetary Affairs	PSE ETTL Harald	24/01/2007
ENVI Environment, Public Health and Food Safety	The committee decided not to give an opinion.	
ITRE Industry, Research and Energy	PSE GLANTE Norbert	27/02/2007
IMCO Internal Market and Consumer Protection	The committee decided not to give an opinion.	
TRAN Transport and Tourism	PPE-DE SOMMER Renate	31/01/2007

Council of the European Union

Council configuration	Meeting	Date
General Affairs	2914	08/12/2008
Justice and Home Affairs (JHA)	2783	05/06/2008
Justice and Home Affairs (JHA)	2838	06/12/2007
Justice and Home Affairs (JHA)	2794	19/04/2007

European Commission

Commission DG	Commissioner
Justice and Consumers	FRATTINI Franco

Key events

12/12/2006	Legislative proposal published	COM(2006)0787	Summary

01/02/2007	Committee referral announced in Parliament		
19/04/2007	Resolution/conclusions adopted by Council		Summary
27/06/2007	Vote in committee		Summary
02/07/2007	Committee report tabled for plenary, 1st reading/single reading	A6-0270/2007	
09/07/2007	Debate in Parliament		
10/07/2007	Results of vote in Parliament		
10/07/2007	Decision by Parliament	T6-0325/2007	Summary
06/12/2007	Debate in Council	2838	
08/12/2008	Act adopted by Council after consultation of Parliament		
08/12/2008	End of procedure in Parliament		
23/12/2008	Final act published in Official Journal		

Technical information

Procedure reference	2006/0276(CNS)
Procedure type	CNS - Consultation procedure
Procedure subtype	Legislation
Legislative instrument	Directive
Legal basis	Euratom Treaty A 203; EC Treaty (after Amsterdam) EC 308
Stage reached in procedure	Procedure completed
Committee dossier	LIBE/6/44115

Documentation gateway

Legislative proposal		COM(2006)0787	12/12/2006	EC	Summary
Document attached to the procedure		SEC(2006)1648	12/12/2006	EC	
Document attached to the procedure		SEC(2006)1654	12/12/2006	EC	
European Central Bank: opinion, guideline, report		CON/2007/0011 OJ C 116 26.05.2007, p. 0001	13/04/2007	ECB	Summary
Committee draft report		PE384.638	08/05/2007	EP	
Amendments tabled in committee		PE388.725	15/05/2007	EP	
Committee opinion	ECON	PE386.361	06/06/2007	EP	
Committee opinion	ITRE	PE386.561	12/06/2007	EP	
Committee report tabled for plenary, 1st reading/single reading		A6-0270/2007	02/07/2007	EP	
Text adopted by Parliament, 1st reading/single reading		T6-0325/2007	10/07/2007	EP	Summary
Commission response to text adopted in plenary		SP(2007)4170	29/08/2007	EC	

Follow-up document		SWD(2012)0190	25/06/2012	EC	Summary
Follow-up document		SWD(2013)0318	28/08/2013	EC	Summary

Additional information

National parliaments	IPEX
European Commission	EUR-Lex

Final act

Directive 2008/114
OJ L 345 23.12.2008, p. 0075 Summary

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

PURPOSE: to create a horizontal framework for the identification and designation of European Critical Infrastructures and for the assessment of needs to improve their protection.

PROPOSED ACT: Council Directive.

BACKGROUND: the security and economy of the European Union as well as the well-being of its citizens depends on certain infrastructure and the services they provide. The destruction or disruption of infrastructure providing key services could entail the loss of lives, the loss of property, a collapse of public confidence and moral in the EU. Any such disruptions or manipulations of critical infrastructure (energy, communication, water, food provisioning, health, transport, etc) should, to the extent possible, be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the Member States, their citizens and the European Union.

In order to counteract these potential vulnerabilities the European Council requested in 2004 the development of a European Programme for Critical Infrastructure Protection. Since then, a comprehensive preparatory work has been undertaken, which has included the organisation of relevant seminars, the publication of a Green Paper and discussions with both public and private stakeholders.

With this in mind, an EPCIP Communication has been developed establishing a horizontal framework concerning the protection of critical infrastructures in Europe.

CONTENT: as part of the EPCIP framework dealing specifically with European Critical Infrastructures, it is necessary to include a 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. The proposed Directive establishes the necessary procedure for the identification and designation of European Critical Infrastructure (ECI), and a common approach to the assessment of the needs to improve the protection of such infrastructure.

The ECI Directive lays down the procedure on how to identify and designate ECI:

- The Commission together with the Member States and relevant stakeholders develop cross-cutting and sectoral criteria for the identification of ECI, which are then adopted through the comitology procedure.
- The cross-cutting criteria are developed on the basis of the severity of the disruption or destruction of the CI. The severity of the consequences of the disruption or destruction of a particular infrastructure should be assessed on the basis, where possible, of: public effect (number of population affected); economic effect (significance of economic loss and/or degradation of products or services); environmental effect; political effects; psychological effects.
- Each Member State then identifies those infrastructures which satisfy the criteria.
- Each Member State then notifies the Commission of the critical infrastructures which satisfy the established criteria.
- Following the identification procedure the Commission prepares a draft list of ECI. The draft list is based on the notifications received from the Member States and other relevant information from the Commission. The list is then adopted through comitology.

Furthermore, the proposed Directive only imposes two obligations on the owners/operators of those critical infrastructures, which are designated as European Critical Infrastructures. These include:

1. The establishment of an Operator Security Plan which would identify the ECI owners' and operators' assets and establish relevant security solutions for their protection. Annex 2 of the ECI Directive provides the minimum contents of such OSPs including:

- identification of important assets;

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

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

- Permanent security measures, which identify indispensable security investments and means which cannot be installed by the owner/operator at short notice. This heading will include information concerning general measures; technical measures (including

installation of detection, access control, protection and prevention means); organizational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems.

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

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

Lastly, the Commission shall take appropriate measures to protect information subject to the requirement of confidentiality to which it has access or which is communicated to it by Member States.

For more details concerning the financial implications of this measure, please refer to the financial statement.

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

OPINION OF THE EUROPEAN CENTRAL BANK

The European Central Bank (ECB) received a request from the Council of the European Union for an opinion on a proposal for a directive of the Council on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection. It supports the proposed directive. In particular, the ECB considers it important to ensure that consistent and coordinated actions are taken in different sectors to properly respond to these threats.

The provisions of the proposed directive such as reporting the summary of risks for each sector to the Commission, must respect existing national and EU authorities' competencies. In particular, it will be necessary to ensure that the national provisions implementing the proposed directive will be fully compatible with central banks' oversight powers or obligations with respect to payment, securities clearing and settlement systems and infrastructures, clearing houses and central counterparties. In this respect it is understood that the framework provided by this proposed directive will not prejudice central banks' powers and independence. A recital should be introduced in the proposed directive to reflect these considerations.

Moreover, the ECB stresses that the Eurosystem and/or national central banks have already established measures ensuring business continuity in euro area payment systems, and the ECB considers that this work should be recognised with a view to avoiding duplication and ensuring consistency in the work done by several authorities.

The ECB also made the following comments :

1. the financial sector identified in the proposed directive is sub-divided into (1) payment and securities clearing and settlement infrastructure and systems; and (2) regulated markets. The ECB proposes broader wording to cover trading, payment, clearing and settlement systems and infrastructures for financial instruments;
2. the definition of ?critical infrastructure? expressly recognises cross-sector dependencies since the effectiveness of implementing measures for any one sector could be severely undermined by failure to properly address sectoral interdependencies. However, it is noted that this definition does not expressly refer only to assets located solely within the EU. Therefore, it is not clear how assets located partly outside the EU, whose disruption or destruction would affect European critical infrastructures, would be treated under the proposed directive. The ECB would welcome further clarification of this issue;
3. the ?severity test? relevant to the identification of European critical infrastructures is quite broad and should be enhanced with clearer indications to ensure consistency of designation across countries and sectors. It would be helpful to further clarify this concept when establishing cross-cutting and sectoral criteria through the comitology procedure under the proposed directive. It is noted that the proposed directive is likely to bring additional administrative requirements which are likely to have associated costs for infrastructures and relevant authorities. Depending on the establishment of such thresholds, infrastructures not currently overseen may be caught and subject to additional costs;
4. a separate Community act may be needed to establish procedures to identify and designate ECIs owned or operated by Community institutions, bodies or agencies. While under the proposed directive the Commission may propose a list of critical infrastructures to be designated as ECIs on the basis both of notifications made by Member States and ?of any other information at the Commission's disposal?, it might not be practical for ECIs operated by Community bodies and having a pan-European dimension to be part of a system that would be administered by the Member States;
5. the list of critical infrastructures designated as ECIs is required to be adopted in accordance with the comitology procedure established by the proposed directive. The list of all ECIs would be adopted before the establishment and putting into operation of the OSPs containing relevant security solutions for the protection of the listed ECIs, since operators have a year following designation to draw up an OSP. In this context, publicity is undesirable for payment and securities clearing and settlement infrastructures and systems. In particular, as the purpose of the Directive includes the preparation for threats affecting financial markets, it would be unsound to publicly disclose the list of critical infrastructures materially relevant for the smooth functioning of financial markets. Today, no country in the world would publicly disclose such a list on the basis of similar considerations. The ECB therefore strongly recommends keeping the list of ECIs confidential;
6. lastly, the ECB strongly recommends giving adequate consideration to existing measures in defining implementing measures and focusing on those areas where no specific measures have been so far identified. The ECB would prefer no specific legally binding measures to be adopted. Should the Commission decide to adopt implementing measures, the ECB will have to be formally consulted under the Treaty on any such measures relating to payment and securities clearing and settlement infrastructures and systems, and other matters falling within the ECB's fields of competence

Where the above advice would lead to changes in the proposed directive, the ECB has set out drafting proposals.

In particular, it proposes:

- to include a new recital 17a aiming to take account of the work and regular assessments conducted by the central banks within their fields of competence;

- to make a slight change to Annex 1 on the list of critical infrastructure sectors (VII Financial). The ECB suggests changing the title to ?Trading, payment clearing and settlement infrastructures and systems for financial instruments?. The reference to ?regulated markets? has been deleted.

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

The Council adopted conclusions emphasising that the ultimate responsibility of the Member States for managing arrangements for the protection of critical infrastructures within their national borders. At the same time, the Council reiterates that action at European Community level will add value by supporting and complementing Member States' activities, while respecting the principle of subsidiarity and taking due account of available budgetary resources as defined in the Financial Framework 2007 - 2013. Member States? responsibility includes, with due regard for existing Community competences, risk analysis and threat assessment in relation to European critical infrastructure situated in their territory, interfacing with its owners/operators, and exchanging information with the Commission on a summary basis.

The Council welcomes the efforts of the Commission to develop a European procedure for the identification and designation of European Critical Infrastructure and the assessment of the need to improve its protection. This procedure should be based on adequate definitions and take into account cross-cutting as well as sectoral criteria, with a view to focusing its actions on those infrastructures damage to or destruction of which would have critical consequences. The Council considers in particular that such a procedure, established with due regard for the competences of the Member States and of the Community, could be of added value.

Owners/operators of European Critical Infrastructure, including the private sector, must be actively involved. They should - by a variety of means and arrangements including voluntary measures - take proper measures to protect their infrastructures. Such measures could be security plans and security liaison officers. The costs to owners and operators of taking these measures should be proportionate and reasonable.

The Council stresses that the greatest possible use should be made of recommendations, information sharing and exchange of best practice at EC level in order to promote voluntary protection measures by the owners/operators of European Critical Infrastructures. The Council will examine the added value of further measures with a view to ensuring security standards in the European Union and comparable competition conditions throughout the European Union. The Council stresses the need for any framework to be clear and consistent; duplications of or contradictions between different measures, acts or provisions must be avoided.

Where the exchange of sensitive or classified information in any group or body is indispensable for the implementation of a European Programme for Critical Infrastructure Protection, the provisions set up in the appropriate security procedures and regulations must be strictly observed.

The Council encourages Member States to launch any appropriate action for the protection of critical infrastructures. The Council recognises that existing actions by Member States are conducted through a variety of means and will pay particular attention to the question of how future measures for protecting European Critical Infrastructures can enable this approach to continue under a common framework. Member States may decide to take up the Commission's offer to provide critical infrastructure protection relevant support and research results generated at EC level or by Member States.

The Council intends to continue its discussion about the Commission communication including the Action plan and the Commission proposal for a Directive in the spirit of the abovementioned conclusions.

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

The Committee on Civil Liberties, Justice and Home Affairs adopted by a large majority the report by Jeanine HENNIS-PLASSCHAERT (ALDE, NL) amending, under the consultation procedure, the proposal for a Council Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection.

The main amendments are as follows:

- the title of the proposal is amended to underline that it concerns ?priority sectors? as opposed to ?all? sectors;

- structurally conditioned threats should also be identified, but the threat of terrorism should be given priority;

- reinforce the principle according to which the directive strengthens public safety through a consistent and efficient system that is not at cross-purposes with itself;

- there are a number of critical infrastructures in the Community, the disruption of which would affect three or more Member States or at least two other Member States other than that in which the critical infrastructure is located. This may include transboundary cross-sector effects resulting from interdependencies between interconnected infrastructure. Such European critical infrastructure should be identified by means of a common procedure. On the basis of common criteria a list of priority sectors with European critical infrastructure should be drawn up. A common action framework should be laid down for the protection of such European critical infrastructures that puts Member States in a position to reduce the potential danger to critical infrastructure on their territory by taking appropriate measures. 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;

- a series of measures governing the identification, designation and protection of critical infrastructures already exists for some sectors. Any

future Community-wide regulation should not result in duplicate regulation in these sectors in the absence of added security;

- Critical infrastructure should be designed in a way that minimises any links with and localisation in third countries. The localisation of elements of critical infrastructures outside the European Union increases the risk of terrorist attacks with spill-over effects on the whole infrastructure, access by terrorists to data stored outside the European Union, as well as risks of non-compliance with Community legislation, thus rendering the entire infrastructure more vulnerable. The recent SWIFT case showed that critical data needs to be protected against illegal use by foreign authorities or private actors;

- each owner/operator of European critical infrastructure should establish an Operator Security Plan identifying critical assets and laying down relevant security solutions for their protection. It should take into account vulnerability, threat and risk assessments, as well as other relevant information provided by Member State authorities;

- these Operator Security Plans should be forwarded to the CIP Contact Point in the Member States. Compliance with existing sector-based protection measures could satisfy the requirement to establish and update an Operator Security Plan as well as designate a Security Liaison Officer;

- this Directive complements existing sectoral measures at Community level and in the Member States. Where Community mechanisms and legislation are already in place, they should be implemented and applied so as to contribute to the improvement of public safety. In so doing, overlaps and contradictions with this Directive and the imposition of additional costs without an additional gain in security are to be avoided;

- as regards proportionality, particular attention should be paid to financial acceptability for owners or operators and for the Member States;

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

- the cross-cutting and sectoral criteria to be used to identify European Critical Infrastructures shall be built on existing protection criteria and be adopted and amended in accordance with Article 308 of the EC Treaty and Article 203 of the Euratom Treaty;

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

- each Member State shall identify the priority sectors within its territory, as well as those outside its territory that may have an impact on it;

- each Member State shall notify the Commission of the priority sectors thus identified at the latest one year after the adoption of the relevant criteria and thereafter on an on-going basis;

- the list of priority sectors with critical infrastructure shall be adopted and amended by the Council;

- Data protection: the processing of personal data carried out directly or through an intermediary by, and necessary for the activities of, European Critical Infrastructures shall be carried out in accordance with the provisions of Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and of the applicable principles with regard to data protection. The data processing shall be carried out within the EU and any mirroring of data shall not be allowed in third countries for reasons of security;

- the Commission and the Council shall adopt a list of existing protection measures applicable to specific sectors listed in Annex I. Compliance with one or more of the listed protection measures satisfies the requirement to establish and update an Operator Security Plan;

- each Member State shall report to the Commission on a summary basis on the types of structural vulnerabilities, threats and risks encountered in European Critical Infrastructures within 12 months (as opposed to 18 months) following the adoption of the list and thereafter on an ongoing basis every 2 years;

- a common template for these reports shall be developed by the Commission and approved by the Council;

- extension of the transposition deadline is essential since transposition by the end of 2007 is unrealistic therefore Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 31 December 2008 at the latest. They shall forthwith communicate to the Commission the text of those provisions and a correlation table between those provisions and this Directive.

Lastly, MEPs have decided to make a list of ?possible? critical infrastructure sectors to be taken into account when setting up the definitive list. Radio communication and navigation Radio communication, navigation and radio-frequency identification (RFID) spectres; Payment and securities clearing and settlement infrastructures and systems and their service providers and banking and insurance.

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

The European Parliament adopted the resolution by Jeanine HENNIS-PLASSCHAERT (ALDE, NL) amending the proposal for a Council Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection. The Parliament stressed that responsibility for protecting critical infrastructure still rests primarily with Member States and private stakeholders.

The Parliament endorsed the amendments tabled by the competent committee.

The main amendments are as follows:

- the title of the proposal is amended to underline that it concerns ?priority sectors? as opposed to ?all? sectors;
- structurally conditioned threats should also be identified, but the threat of terrorism should be given priority;
- reinforce the principle according to which the directive strengthens public safety through a consistent and efficient system that is not at cross-purposes with itself;
- there are a number of critical infrastructures in the Community, the disruption of which would affect three or more Member States or at least two other Member States other than that in which the critical infrastructure is located. This may include transboundary cross-sector effects resulting from interdependencies between interconnected infrastructure. Such European critical infrastructure

should be identified by means of a common procedure. On the basis of common criteria a list of priority sectors with European critical infrastructure should be drawn up. A common action framework should be laid down for the protection of such European critical infrastructures that puts Member States in a position to reduce the potential danger to critical infrastructure on their territory by taking appropriate measures. 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;

- a series of measures governing the identification, designation and protection of critical infrastructures already exists for some sectors. Any future Community-wide regulation should not result in duplicate regulation in these sectors in the absence of added security;
- each owner/operator of European critical infrastructure should establish an Operator Security Plan identifying critical assets and laying down relevant security solutions for their protection. It should take into account vulnerability, threat and risk assessments, as well as other relevant information provided by Member State authorities;
- these Operator Security Plans should be forwarded to the CIP Contact Point in the Member States. Compliance with existing sector-based protection measures could satisfy the requirement to establish and update an Operator Security Plan as well as designate a Security Liaison Officer;
- this Directive complements existing sectoral measures at Community level and in the Member States. Where Community mechanisms and legislation are already in place, they should be implemented and applied so as to contribute to the improvement of public safety. In so doing, overlaps and contradictions with this Directive and the imposition of additional costs without an additional gain in security are to be avoided;
- as regards proportionality, particular attention should be paid to financial acceptability for owners or operators and for the Member States;
- ?European Critical Infrastructure? means critical infrastructures the disruption or destruction of which would significantly affect three or more Member States, or at least two Member States if the critical infrastructure is located in another Member State. This includes effects resulting from cross-sector dependencies on other types of infrastructure;
- the cross-cutting and sectoral criteria to be used to identify European Critical Infrastructures shall be built on existing protection criteria and be adopted and amended in accordance with Article 308 of the EC Treaty and Article 203 of the Euratom Treaty;
- where Community mechanisms are already in place, they shall continue to be used. Duplications of, or contradictions between, different acts or provisions shall be avoided at all costs;
- each Member State shall notify the Commission of the priority sectors thus identified at the latest one year after the adoption of the relevant criteria and thereafter on an on-going basis;
- each Member State shall report to the Commission on a summary basis on the types of structural vulnerabilities, threats and risks encountered in European Critical Infrastructures within 12 months (as opposed to 18 months) following the adoption of the list and thereafter on an ongoing basis every 2 years;
- a common template for these reports shall be developed by the Commission and approved by the Council;
- extension of the transposition deadline from December 2007 to December 2008.

Lastly, MEPs have decided to make a list of ?possible? critical infrastructure sectors to be taken into account when setting up the definitive list. Radio communication and navigation Radio communication, navigation and radio-frequency identification (RFID) spectres; Payment and securities clearing and settlement infrastructures and systems and their service providers and banking and insurance.

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

PURPOSE: to create a horizontal framework for the identification of European Critical Infrastructures.

LEGISLATIVE ACT: Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

CONTENT: the Council adopted this Directive following political agreement reached in June 2008. The Directive establishes a procedure for the identification and designation of European critical infrastructures (?ECIs?), and a common approach to the assessment of the need to improve the protection of such infrastructures in order to contribute to the protection of people. It focuses on the energy and transport sectors.

?European critical infrastructure? or ?ECI? is defined as critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least 2 Member States. The significance of the impact will be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure.

In the Annex, the Directive details the types of infrastructures concerned:

Energy

- electricity Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity;
- oil production, refining, treatment, storage and transmission by pipelines;
- gas production, refining, treatment, storage and transmission by pipelines, LNG terminals.

Transport

- road transport
- rail transport
- air transport
- inland waterways transport
- ocean and short-sea shipping and ports.

Evaluation method: ECIs should be identified and designated by means of a common procedure. The evaluation of security requirements for such infrastructures should be done under a common minimum approach. Each Member State must identify potential ECIs which both satisfy cross-cutting and sectoral criteria. The Directive requires each Member State to identify the critical infrastructures which may be designated as an ECI. This procedure shall be implemented by each Member State through the following series of consecutive steps (Annex III).

- Step 1: each Member State shall apply the sectoral criteria in order to make a first selection of critical infrastructures within a sector.
- Step 2: each Member State shall apply the definition of critical infrastructure to the potential ECI identified under step 1.
- Step 3: each Member State shall apply the transboundary element of the definition of ECI to the potential ECI.
- Step 4: each Member State shall apply the cross-cutting criteria to the remaining potential ECIs.

The cross-cutting criteria shall take into account: the severity of impact; and, for infrastructure providing an essential service, the availability of alternatives; and the duration of disruption/recovery. A potential ECI which does not satisfy the cross-cutting criteria will not be considered to be an ECI. A potential ECI which has passed through this procedure shall only be communicated to the Member States which may be significantly affected by the potential ECI.

The cross-cutting criteria shall comprise the following:

- casualties criterion (assessed in terms of the potential number of fatalities or injuries);
- economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects);
- public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services).

The sectoral criteria shall take into account the characteristics of individual ECI sectors.

Identification: the process of identifying and designating must be completed by 12 January 2011 and reviewed on a regular basis.

The Member State on whose territory a designated ECI is located shall inform the Commission on an annual basis of the number of designated ECIs per sector and of the number of Member States dependent on each designated ECI. Only those Member States that may be significantly affected by an ECI shall know its identity. The Member States on whose territory an ECI is located shall inform the owner/operator of the infrastructure concerning its designation as an ECI. Information concerning the designation of an infrastructure as an ECI shall be classified at an appropriate level.

Operator security plans: the operator security plan (?OSP?) procedure must identify the critical infrastructure assets of the ECI and which security solutions exist or are being implemented for their protection. The minimum content to be addressed by an ECI OSP procedure is set out in Annex II, and includes conducting a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact.

Security Liaison Officers: the Security Liaison Officer functions as the point of contact for security related issues between the owner/operator of the ECI and the relevant Member State authority.

Commission support for ECIs: the Commission will support the owners/operators of designated ECIs by providing access to available best practices and methodologies as well as support training and the exchange of information on new technical developments related to critical infrastructure protection.

Sensitive European critical infrastructure protection-related information: the act provides that any person handling classified information pursuant to this Directive on behalf of a Member State or the Commission must have an appropriate level of security vetting. Member States, the Commission and relevant supervisory bodies shall ensure that sensitive European critical infrastructure protection-related information submitted to the Member States or to the Commission is not used for any purpose other than the protection of critical infrastructures.

Review: a review of this Directive shall begin on 12 January 2012. If deemed appropriate and in conjunction with the review, subsequent sectors to be used for the purpose of implementing this Directive may be identified. Priority shall be given to the ICT sector.

Implementation: 12/01/2011.

ENTRY INTO FORCE: 12/01/2009.

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

This document presents the main preliminary findings of the review of the European Programme for Critical Infrastructure Protection (EPCIP) and in particular Directive 2008/114/EC on the identification and designation of European Critical Infrastructures.

It provides a general analysis of the elements of the critical infrastructure protection programme and describes the on-going development of risk assessment methodology in this field.

In addition, it contains the required annual reporting on EPCIPs external dimension.

The report states that the review of the different EPCIP elements so far implemented has already led to a number of important findings for the preparation of a reshaped CIP policy package. All Member States have legally implemented Directive 2008/114/EC by establishing a process to identify and designate European Critical Infrastructures, which has contributed to raising CIP awareness in the EU and in the Member States. Furthermore, although there is evidence that the Directive has also helped in assessing the need to improve the protection of European critical infrastructures in the transport and energy sectors, there is no indication that it has actually improved security in these sectors.

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

This Commission staff working document sets out a new approach to the European Programme for Critical Infrastructure Protection (EPCIP) with a view to making them more secure. It builds on a comprehensive review of the 2006 European Programme for Critical Infrastructure Protection and the Council Directive 2008/114/EC, conducted in close cooperation with EU Member States and stakeholders.

The review process of the current EPCIP revealed that there has not been enough consideration of the links between critical infrastructures in different sectors, nor indeed across national boundaries.

In order to properly protect Europes critical infrastructures, and in order to build their resilience, a new approach to tackle this gap is needed. To pilot the new approach, the Commission will start by working with four critical infrastructures of European dimension: Eurocontrol, Galileo, the electricity transmission grid and the gas transmission network (the Four). It is expected that other relevant infrastructures could then benefit from the processes and tools developed when carrying out the work with the Four. Through work with the Four and developing the new approach, the EU can both play a supporting role for Member States in their own CI protection and resilience work and facilitate better cooperation on CI protection and resilience within the EU. Given that many critical infrastructures are privately owned, better cooperation includes supporting the development of private-public structured dialogues.

The first stage will be to work with the Four to ensure a comprehensive understanding of their CIP measures to date in each of the prevention, preparedness and response work streams, including looking at how interdependencies and cascading effects feed into their CIP planning. The next step will be to identify common factors and consider ways in which their CI protection and resilience measures can be improved.