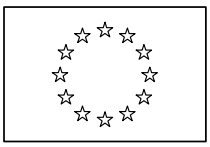

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 12.12.2006
COM(2006) 786 final

COMMUNICATION FROM THE COMMISSION

on a European Programme for Critical Infrastructure Protection

COMMUNICATION FROM THE COMMISSION

on a European Programme for Critical Infrastructure Protection

(Text with EEA relevance)

1. BACKGROUND

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

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

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

The 2005 December Justice and Home Affairs (JHA) Council Conclusions on Critical Infrastructure Protection called upon the Commission to make a proposal for a European Programme for Critical Infrastructure Protection.

This Communication sets out the principles, processes and instruments proposed to implement EPCIP. The implementation of EPCIP will be supplemented where relevant by sector specific Communications setting out the Commission's approach concerning particular critical infrastructure sectors[1].

2. PURPOSE, PRINCIPLES AND CONTENT OF EPCIP

2.1. The objective of EPCIP

The general objective of EPCIP is to improve the protection of critical infrastructures in the EU. This objective will be achieved by the creation of an EU framework concerning the protection of critical infrastructures which is set out in this Communication.

[1] The Commission intends to put forward a Communication on Protecting Europe's Critical Energy and Transport Infrastructure.

2.2. Types of threats to be addressed by EPCIP

While recognising the threat from terrorism as a priority, the protection of critical infrastructure will be based on an all-hazards approach. If the level of protective measures in a particular CI sector is found to be adequate, stakeholders should concentrate their efforts on threats to which they are vulnerable.

2.3. Principles

The following key principles will guide the implementation of EPCIP:

- **Subsidiarity** – The Commission's efforts in the CIP field will focus on infrastructure that is critical from a European, rather than a national or regional perspective. Although focusing on European Critical Infrastructures, the Commission may where requested and taking due account of existing Community competences and available resources provide support to Member States concerning National Critical Infrastructures.

- **Complementarity** - the Commission will avoid duplicating existing efforts, whether at EU, national or regional level, where these have proven to be effective in protecting critical infrastructure. EPCIP will therefore complement and build on existing sectoral measures.

- **Confidentiality** - Both at EU level and MS level, Critical Infrastructure Protection Information (CIPI) will be classified appropriately and access granted only on a need-to-know basis. Information sharing regarding CI will take place in an environment of trust and security.

- **Stakeholder Cooperation** – All relevant stakeholders will, as far as possible, be involved in the development and implementation of EPCIP. This will include the owners/operators of critical infrastructures designated as ECI as well as public authorities and other relevant bodies.

- **Proportionality** – measures will only be proposed where a need has been identified following an analysis of existing security gaps and will be proportionate to the level of risk and type of threat involved.

- **Sector-by-sector approach** – Since various sectors possess particular experience, expertise and requirements with CIP, EPCIP will be developed on a sector-by-sector basis and implemented following an agreed list of CIP sectors.

2.4. The EPCIP framework

The framework will consist of:

- A procedure for the identification and designation of European Critical Infrastructures (ECI), and a common approach to the assessment of the needs to improve the protection of such infrastructures. This will be implemented by way of a Directive.

- Measures designed to facilitate the implementation of EPCIP including an EPCIP Action Plan, the Critical Infrastructure Warning Information Network (CIWIN),

the use of CIP expert groups at EU level, CIP information sharing processes and the identification and analysis of interdependencies.

- Support for Member States concerning National Critical Infrastructures (NCI) which may optionally be used by a particular Member State. A basic approach to protecting NCI is set out in this Communication.

- Contingency planning.

- An external dimension.

- Accompanying financial measures and in particular the proposed EU programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013, which will provide funding opportunities for CIP related measures having a potential for EU transferability.

Each of these measures is addressed below.

2.5. The CIP Contact Group

An EU level mechanism is required in order to serve as the strategic coordination and cooperation platform capable of taking forward work on the general aspects of EPCIP and sector specific actions. Consequently, a CIP Contact Group will be created.

The CIP Contact Group will bring together the CIP Contact Points from each Member State and will be chaired by the Commission. Each Member State should appoint a CIP Contact Point who would coordinate CIP issues within the Member State and with other Member States, the Council and the Commission. The appointment of the CIP Contact Point would not preclude other authorities in the Member State from being involved in CIP issues.

3. EUROPEAN CRITICAL INFRASTRUCTURES (ECI)

European Critical Infrastructures constitute those designated critical infrastructures which are of the highest importance for the Community and which if disrupted or destroyed would affect two or more MS, or a single Member State if the critical infrastructure is located in another Member State. This includes transboundary effects resulting from interdependencies between interconnected infrastructures across various sectors. The procedure for the identification and designation of European Critical Infrastructures (ECI), and a common approach to the assessment of the needs to improve the protection of such infrastructures will be established by means of a Directive.

4. MEASURES DESIGNED TO FACILITATE THE DEVELOPMENT AND IMPLEMENTATION OF EPCIP

A number of measures will be used by the Commission to facilitate the implementation of EPCIP and to further EU level work on CIP.

4.1. EPCIP Action Plan

EPCIP will be an ongoing process and regular review will be carried out in the form of the EPCIP Action Plan (Annex). The Action Plan will set out the actions to be achieved along with relevant deadlines. The Action Plan will be updated regularly based on the progress made.

The EPCIP Action Plan organizes CIP related activities around three work streams:

- Work Stream 1 which will deal with the strategic aspects of EPCIP and the development of measures horizontally applicable to all CIP work.
- Work Stream 2 dealing with European Critical Infrastructures and implemented at a sectoral level.
- Work Stream 3 which will support the Member States in their activities concerning National Critical Infrastructures.

The EPCIP Action Plan will be implemented taking into account sector specificities and involving, as appropriate, other stakeholders.

4.2. Critical Infrastructure Warning Information Network (CIWIN)

The Critical Infrastructure Warning Information Network (CIWIN) will be set up through a separate Commission proposal and due care will be taken to avoid duplication. It will provide a platform for the exchange of best practices in a secure manner. CIWIN will complement existing networks and could also provide an optional platform for the exchange of rapid alerts linked to the Commission's ARGUS system. The necessary security accreditation of the system will be undertaken in line with relevant procedures.

4.3. Expert groups

Stakeholder dialogue is crucial for improving the protection of critical infrastructures in the EU. Where specific expertise is needed the Commission may therefore setup CIP expert groups at EU level to address clearly defined issues and to facilitate public-private dialogue concerning critical infrastructure protection. Expert groups will support EPCIP by facilitating exchanges of views on related CIP issues on an advisory basis. These expert groups constitute a voluntary mechanism in which public and private resources are blended to achieve a goal or set of goals judged to be of mutual benefit both to citizens and the private sector.

CIP expert groups will not replace other existing groups already established or which could be adapted to fulfil the needs of EPCIP, nor will they interfere with direct information exchanges between industry, the MS authorities and the Commission.

An EU level CIP expert group will have a clearly stated objective, a timeframe for the objective to be achieved and clearly identified membership. CIP Expert Groups will be dissolved following the achievement of their objectives.

Specific functions of CIP expert groups may vary across CI sectors depending on the unique characteristics of each sector. These functions may include the following tasks:

- Assist in identifying vulnerabilities, interdependencies and sectoral best practices;

- Assist in the development of measures to reduce and/or eliminate significant vulnerabilities and the development of performance metrics;

- Facilitating CIP information-sharing, training and building trust;

- Develop and promote "business cases" to demonstrate to sector peers the value of participation in infrastructure protection plans and initiatives;

- Provide sector-specific expertise and advice on subjects such as research and development.

4.4. The CIP information sharing process

The CIP information sharing process among relevant stakeholders requires a relationship of trust, such that the proprietary, sensitive or personal information that has been shared voluntarily will not be publicly disclosed and that that sensitive data is adequately protected. Care must be taken to respect privacy rights.

Stakeholders will take appropriate measures to protect information concerning such issues as the security of critical infrastructures and protected systems, interdependency studies and CIP related vulnerability, threat and risks assessments. Such information will not be used other than for the purpose of protecting critical infrastructure. Any personnel handling classified information will have an appropriate level of security vetting by the Member State of which the person concerned is a national.

In addition, CIP information exchange will recognize that certain CIP information, though unclassified, may still be sensitive and therefore needs to be treated with care.

CIP information exchange will facilitate the following:

- Improved and accurate information and understanding about interdependencies, threats, vulnerabilities, security incidents, countermeasures and best practices for the protection of CI;

- Increased awareness of CI issues;

- Stakeholder dialogue;

- Better-focused training, research and development.

4.5. Identification of interdependencies

The identification and analysis of interdependencies, both geographic and sectoral in nature, will be an important element of improving critical infrastructure protection in the EU. This ongoing process will feed into the assessment of vulnerabilities, threats and risks concerning critical infrastructures in the EU.

5. NATIONAL CRITICAL INFRASTRUCTURES (NCI)

With due regard to existing Community competences, the responsibility for protecting National Critical Infrastructures falls on the NCI owners/operators and on the Member States. The Commission will support the Member States in these efforts where requested to do so.

With a view to improving the protection of National Critical Infrastructures each Member State is encouraged to establish a National CIP Programme. The objective of such programmes would be to set out each Member State's approach to the protection of National Critical Infrastructures located within its territory. Such programmes would at a minimum address the following issues:

- The identification and designation by the Member State of National Critical Infrastructures according to predefined national criteria. These criteria would be developed by each Member State taking into account as a minimum the following qualitative and quantitative effects of the disruption or destruction of a particular infrastructure:

    - Scope - The disruption or destruction of a particular critical infrastructure will be rated by the extent of the geographic area which could be affected by its loss or unavailability.

    - Severity - The consequences of the disruption or destruction of a particular infrastructure will be assessed on the basis of:

    – Public effect (number of population affected);

    – Economic effect (significance of economic loss and/or degradation of products or services);

    – Environmental effect;

    – Political effects;

    – Psychological effects;

    – Public health consequences.

    Where such criteria do not exist, the Commission will assist a Member State, at its request, in their development by providing relevant methodologies.

- The establishment of a dialogue with CIP owners/operators.

- Identification of geographic and sectoral interdependencies.

- Drawing-up NCI related contingency plans where deemed relevant.

- Each Member State is encouraged to base its National CIP Programme on the common list of CI sectors established for ECI.

The introduction of similar approaches to the protection of NCI in the Member States would contribute to ensuring that CI stakeholders throughout Europe benefit from not being

subjected to varying frameworks resulting in additional costs and that the Internal Market is not distorted.

6. CONTINGENCY PLANNING

Contingency planning is a key element of the CIP process so as to minimize the potential effects of a disruption or destruction of a critical infrastructure. The development of a coherent approach to the elaboration of contingency plans addressing such issues as the participation of owners/operators of critical infrastructure, cooperation with national authorities and information sharing among neighbouring countries should form an important element of the implementation of the European Programme for Critical Infrastructure Protection.

7. EXTERNAL DIMENSION

Terrorism, other criminal activities, natural hazards and other causes of accidents are not constrained by international borders. Threats cannot be seen in a purely national context. Consequently, the external dimension of Critical Infrastructure Protection needs to be fully taken in to account in the implementation of EPCIP. The interconnected and interdependent nature of today's economy and society means that even a disruption outside of the EU's borders may have a serious impact on the Community and its Member States. Equally true, the disruption or destruction of a critical infrastructure within the EU may have a detrimental effect on the EU's partners. Finally, working toward the goal of increasing the protection of critical infrastructure within the EU will minimize the risk of the EU economy being disrupted and thereby contribute to the EU's global economic competitiveness.

Consequently, enhancing CIP cooperation beyond the EU through such measures as sector specific memoranda of understanding (e.g. on the development of common standards, undertaking joint CIP related studies, identification of common types of threats and exchanging best-practices on protection measures) and encouraging the raising of CIP standards outside of the EU should therefore be an important element of EPCIP. External cooperation on CIP will primarily focus on the EU's neighbours. Given however the global interconnectedness of certain sectors including ICT and financial markets, a more global approach would be warranted. Dialogue and the exchange of best practices should nevertheless involve all relevant EU partners and international organizations. The Commission will also continue promoting improvements in the protection of critical infrastructures in non-EU countries by working with G8, Euromed and European Neighbourhood Policy partners through existing structures and policies, including the "Instrument for Stability".

8. ACCOMPANYING FINANCIAL MEASURES

The Community programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013 will contribute to the implementation of EPCIP.

Within the general objectives, and unless covered by other financial instruments, the programme will stimulate, promote and develop measures on prevention, preparedness and

consequence management aimed at preventing or reducing all security risks, in particular risks linked with terrorism, where appropriate based on comprehensive threat and risk assessments.

Funding under the programme, by way of grants and Commission initiated actions, will be used in particular toward the development of instruments, strategies, methodologies, studies, assessments and activities/measures in the field of the effective protection of critical infrastructure (at both EU and MS levels).

ANNEX

EPCIP Action Plan

Work Stream 1. Consecutive EPCIP strategies

Work stream 1 will serve as the strategic platform for overall EPCIP coordination and cooperation through the EU CIP Contact Group.

Phase 1

Action	Actor	Timeframe
Identification of priority sectors for action (The transport and energy sectors will be among the first priorities)	Commission	As soon as possible and thereafter on an annual basis
Development of common CI sector-based working definitions and terminology	Commission, MS and other stakeholders where relevant	at the latest one year following the entry into force of the ECI Directive
Elaboration of general criteria to be used in identifying ECI	Commission, MS and other stakeholders where relevant	at the latest one year following the entry into force of the ECI Directive
Creation of an inventory of existing national, bilateral and EU critical infrastructure protection programmes	Commission, MS	ongoing
Creation and agreement on guidelines on collection and use of sensitive data between stakeholders	Commission, MS, and other stakeholders where relevant	ongoing
Collection of CIP related best practices, risk assessment tools and methodologies	Commission, MS and other stakeholders where relevant	ongoing
Commissioning studies concerning interdependencies	Commission, MS and other stakeholders where relevant	ongoing

Phase 2

Action	Actor	Timeframe
Identification of gaps where Community initiatives would have added-value	Commission, MS and other stakeholders where relevant	ongoing
Where relevant, setting up of CIP sector based expert groups at EU level	Commission, MS and other stakeholders where relevant	ongoing
Identification of proposals for CIP actions that could be funded at EU level	Commission, MS	ongoing
Initiation of EU funding for CIP actions	Commission	ongoing

Phase 3

Action	Actor	Timeframe
Initiation of cooperation with 3rd countries and international organisations;	Commission, MS	ongoing

Work Stream 2. Protection of European critical infrastructure (ECI)

Work stream 2 will focus on reducing the vulnerability of ECI.

Phase 1

Action	Actor	Timeframe
Elaboration of sector specific criteria to be used in identifying ECI	Commission, MS and other stakeholders where relevant	at the latest one year following the entry into force of the ECI Directive

Phase 2

Action	Actor	Timeframe
Identification and verification on a sector-by-sector basis of CI likely to qualify as ECI	Commission, MS	at the latest one year after the adoption of the relevant criteria and thereafter on an ongoing basis
Designation of ECI	Commission, MS	ongoing

Identification of vulnerabilities, threats and risks to particular ECI including the establishment of Operator Security Plans (OSPs)	Commission, MS, ECI owners/operators (generic report to Commission)	at the latest one year after designation as ECI
Assessment of whether protection measures are needed and whether EU level measures are required	Commission, MS and other stakeholders where relevant	at the latest 18 months after designation as ECI
Assessment of the approach of each Member State to alert levels concerning infrastructure designated as ECI. Launching of a feasibility study on calibrating or harmonizing such alerts.	Commission, MS	ongoing

Phase 3

Action	Actor	Timeframe
Development and adoption of proposals for minimum protection measures concerning ECI	Commission, MS, ECI owners/operators	following the assessment of whether protection measures are needed and whether EU level measures are required
Implementation of minimum protection measures	MS, ECI owners/operators	ongoing

Work Stream 3. Support concerning NCI

Work Stream 3 is an intra-Member State work stream to assist the Member States in the protection of NCI.

Phase 1

Action	Actor	Timeframe
Exchange of information on the criteria used to identify NCI	MS (Commission may assist where requested)	ongoing

Phase 2

Action	Actor	Timeframe
Identification and verification on a sector-by-sector basis of CI likely to qualify as NCI	MS and other stakeholders where relevant	ongoing
Designation of particular CI as NCI	MS	ongoing
Analysis of existing security gaps in relation to NCI on a sector-by-sector basis	MS and other stakeholders where relevant (Commission may assist where requested)	ongoing

Phase 3

Action	Actor	Timeframe
Establishment and development of National CIP Programmes	MS (Commission may assist where requested)	ongoing
Development of specific protection measures for each NCI	MS, NCI (Commission may assist where requested)	ongoing
Monitoring that owners/operators carry out the necessary implementation measures	MS	ongoing