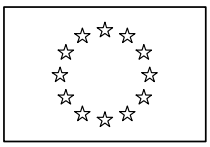

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 17.11.2005
COM(2005) 576 final

GREEN PAPER

ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION

(presented by the Commission)

GREEN PAPER

ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION

1. BACKGROUND

Critical infrastructure (CI) can be damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, accidents or computer hacking, criminal activity and malicious behaviour. To save the lives and property of people at risk in the EU from terrorism, natural disasters and accidents, any disruptions or manipulations of CI should, to the extent possible, be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the Member States (MS), their citizens and the European Union. The recent terrorist attacks in Madrid and London have highlighted the risk of terrorist attacks against European infrastructure. The EU's response must be swift, coordinated and efficient.

The European Council of June 2004 asked the Commission to prepare an overall strategy to protect critical infrastructure. In response, the Commission adopted on 20 October 2004 a Communication "Critical Infrastructure Protection in the Fight Against Terrorism" putting forward clear suggestions on what would enhance European prevention, preparedness and response to terrorist attacks involving critical infrastructures.

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 set-up by the Commission of a Critical Infrastructure Warning Information Network (CIWIN).

The Commission has organized two seminars and invited the submission of ideas and comments by MS. The 1st EU Critical Infrastructure Protection Seminar was held on 6-7 June 2005 with the MS participation. Following this seminar, the MS provided the Commission with relevant background papers concerning their approach to CIP and commented on the ideas discussed at the seminar. Submissions were received in June and July, and formed the basis for further CIP development. The 2nd EU CIP seminar was held on 12-13 September in order to advance the discussion on CIP issues. Both MS and industry associations participated in this Seminar. As a result the Commission has decided to put forward this green paper outlining the options for EPCIP.

2. OBJECTIVE OF THE GREEN PAPER

The main objective of the green paper is to receive feedback concerning possible EPCIP policy options by involving a broad number of stakeholders. The effective protection of critical infrastructure requires communication, coordination, and cooperation nationally and at EU level among all interested parties - the owners and operators of infrastructure, regulators, professional bodies and industry associations in cooperation with all levels of government, and the public.

The Green Paper provides options on how the Commission may respond to the Council's request to establish EPCIP and CIWIN and constitutes the second phase of a consultation process concerning the establishment of a European Programme for Critical Infrastructure Protection. The Commission expect that by presenting this green paper, it will receive concrete feedback concerning the policy options outlined in this document. Depending on the outcome of the consultation process, an EPCIP policy package could be put forward during 2006.

3. PURPOSE AND SCOPE OF EPCIP

3.1. The overall goal of EPCIP

The goal of EPCIP would be to ensure that there are adequate and equal levels of protective security on critical infrastructure, minimal single points of failure and rapid, tested recovery arrangements throughout the Union. The level of protection may not be equal for all CIs and may depend on the impact caused by the failure of the CI. EPCIP would be an ongoing process and regular review will be required to keep abreast of new issues and concerns.

EPCIP should minimise as much as possible any negative impact that increased security investments might have on the competitiveness of a particular industry. In calculating the proportionality of the cost, one must not lose sight of the need to maintain stability of markets that is crucial for long-term investment, the influence security has on the evolution of stock markets and on the macro-economic dimension.

Question

Is this an appropriate goal for EPCIP? If not, what should the goal be?

3.2. What should EPCIP protect against

Although consequence management measures are identical or similar for most disruptions, protection measures may differ depending on the nature of the threat. Threats that would significantly diminish abilities to ensure the essential needs and safety of the population, to maintain order and to deliver minimum essential public services or the orderly functioning of the economy, may include intentional attacks and natural disasters. The options are:

a) **an all-hazards approach for everything** – This would be a comprehensive approach taking into account both the threat from intentional attacks as well as natural disasters. It would ensure that synergies between protection measures are exploited to the maximum, but it would not give any particular emphasis to terrorism;

b) **an all-hazards approach with a terrorism priority** - This would be a flexible approach that ensures a link with other types of hazards such as the threat from intentional attacks as well as natural disasters but with terrorism being a priority. If the level of protection measures in a particular industry sector were found to be adequate, stakeholders would concentrate on those threats for which they are still vulnerable.

c) **a terrorism hazards approach** - This would be a terrorism focused approach that would not pay any particular attention to more common threats.

Question
Which approach should EPCIP take? Why?

4. SUGGESTED KEY PRINCIPLES

The following key principles are suggested to form the basis of EPCIP:

- **Subsidiarity** - Subsidiarity would be at the heart of EPCIP, with the protection of critical infrastructure being first and foremost a national responsibility. The prime responsibility for protecting critical infrastructure would fall on the MS and owners/operators acting under a common framework. The Commission would in turn concentrate on aspects related to the protection of critical infrastructures having an EU cross border effect. The responsibility and accountability of owners and operators to make their own decisions and plans for protecting their own assets should not change.

- **Complementarity** - The common EPCIP framework would be complementary to existing measures. Where community mechanisms are already in place, they should continue to be used and will help guarantee the overall implementation of EPCIP.

- **Confidentiality** - Information sharing regarding critical infrastructure protection would take place in an environment of trust and confidentiality. This is a necessity bearing in mind that specific facts about a critical infrastructure asset can be used to cause failure or unacceptable consequences for critical infrastructure installations. Both at EU level and MS level CIP information would be classified and access granted only on a need-to-know basis.

- **Stakeholder Cooperation** – All stakeholders including MS, Commission, industry/business associations, standardisation bodies and owners, operators and users ('users' being defined as organizations that exploit and use the infrastructure for business and service provision purposes) have a role to play in protecting CI. All stakeholders should cooperate and contribute to the development and implementation of EPCIP according to their specific roles and responsibilities. MS authorities would provide leadership and coordination in developing and implementing a nationally consistent approach to the protection of critical infrastructure within their jurisdictions. The owners, operators and users would be actively involved at both the national and EU level. Where sectoral standards do not exist or where international norms have not yet been established, standardisation organisations could adopt common standards where appropriate.

- **Proportionality** - Protection strategies and measures would be proportionate to the level of risk involved as not all infrastructures can be protected from all threats (for example, electricity transmission networks are too large to fence or guard). By applying appropriate risk management techniques, attention would be focused on areas of greatest risk, taking into account the threat, relative criticality, cost-benefit ratio, the level of protective security and the effectiveness of available mitigation strategies.

Question

Are these key principles acceptable? Are some superfluous? Are there additional ones that should be considered?

Do you agree that protection measures should be proportionate to the level of risk involved as not all infrastructures can be protected from all threats?

5. A COMMON EPCIP FRAMEWORK

The damage or loss of a piece of infrastructure in one MS may have negative effects on several others and on the European economy as a whole. This is becoming increasingly likely as new technologies (e.g. the Internet) and market liberalisation (e.g. in electricity and gas supply) mean that much infrastructure is part of a larger network. In such a situation protection measures are only as strong as their weakest link. This means that a common level of protection may be necessary.

Effective protection requires communication, coordination, and cooperation nationally, at EU level (where relevant) and internationally among all stakeholders. A common EU level framework for the protection of critical infrastructure in Europe could be put in place in order to make sure that each MS is providing adequate and equal levels of protection concerning their critical infrastructure and that the rules of competition within the internal market are not distorted. With a view to supporting the activities of the MS, the Commission would facilitate the identification, exchange and dissemination of best practices on CIP related issues by providing a common framework for the protection of critical infrastructure. The scope of this general framework needs to be considered.

The common EPCIP framework would contain horizontal measures that define the competence and responsibilities of all critical infrastructure protection (CIP) stakeholders, as well as laying the foundation for sector specific approaches. The common framework is meant to complement existing sectoral measures at Community level and in MS in order to provide the maximum possible level of security of critical infrastructure present in the European Union. Work on reaching agreement on a common list of definitions and CI sectors should be prioritised.

As the different sectors containing critical infrastructure are very diverse, it would be difficult to prescribe exactly what criteria should be used to identify and protect all of them in a horizontal framework; this should be carried out on a sector-by-sector basis. Nevertheless, there is a need for a common understanding on certain cross-cutting issues.

It is therefore suggested that the strengthening of CI in the EU is achieved by the setting of a common EPCIP framework, (common objectives, methodologies e.g. for comparisons, interdependencies) exchanging best practices and compliance monitoring mechanisms. Some of the elements which would form part of the common framework would include:

- common CIP principles;
- commonly agreed codes/standards
- common definitions on the basis of which sector specific definitions can be agreed (an indicative list of definitions is included in Annex 1);
- common list of CI sectors (an indicative list of sectors is included in Annex 2);

- CIP priority areas;
- description of the responsibilities of the stakeholders involved;
- agreed benchmarks;
- methodologies to compare and prioritise infrastructure in different sectors.

Such a common framework would also minimise potential distorting effects on the internal market.

The common EPCIP framework could be voluntary or mandatory – or a mixture depending on the issue. Both types of framework could complement existing sectoral and horizontal measures at Community and MS level; however, only a legal framework would provide a strong and enforceable legal basis for a coherent and uniform implementation of measures to protect ECI, as well as defining clearly the respective responsibilities of MS and the Commission. Non-binding voluntary measures, while flexible, would not provide clarity on who does what.

Depending on the outcome of a careful analysis and paying due regard to the proportionality of proposed measures, the Commission may make use of a number of instruments, including legislation, in its EPCIP proposal. Impact assessments will accompany proposals for specific measures, where relevant.

Questions

Would a common framework be effective in strengthening CIP?

If a legislative framework is required, what elements should it contain?

Do you agree that the criteria for identifying different types of ECI, and the protection measures considered necessary, should be identified sector-by-sector?

Would a common framework be helpful in clarifying the responsibilities of the stakeholders concerned? To what extent should such a common framework be obligatory and to what extent voluntary?

What should be the scope of the common framework? Do you agree with the list of indicative terms and definitions in annex I on the basis of which, sector specific definitions (where relevant) can be created? Do you agree with the list of indicative CI sectors in annex II?

6. EU CRITICAL INFRASTRUCTURES (ECI)

6.1. Definition of EU critical infrastructure

The definition of what constitutes an EU critical infrastructure would be determined by its cross border effect which ascertains whether an incident could have a serious impact beyond the territory of a MS where the installation is located. Another element to take into account here is the fact that bilateral CIP cooperation schemes between MS constitute a well established and efficient means of dealing with CI between the borders of two MS. Such cooperation would be complementary to EPCIP.

ECI could include those physical resources, services, information technology facilities, networks and infrastructure assets, which, if disrupted or destroyed would have a serious impact on the health, safety, security, economic or social well-being of either:

(a) two or more MS - **this would include certain bilateral CI (where relevant);**

(b) involve three or more MS **- this would exclude all bilateral CI;**

When considering the respective merits of these options it is important to bear the following points in mind:

– the fact that a piece of infrastructure would be designated as ECI, does not mean that it would necessarily require any additional protection measures. The existing protection measures, which could include bilateral agreements between MS, may be perfectly adequate and hence unchanged by a designation as ECI;

– option (a) may involve a higher number of designations;

– option (b) may mean that for infrastructure of concern to only two MS, there would be no Community role even if the level of protection was considered inadequate by one of those two MS and the other MS refused to take action. Option (b) could also lead to a multitude of bilateral agreements or disagreements between MS. Industry, which often operates at a pan-European level, may have to work with a diverse patchwork of different agreements, which may introduce additional costs.

Moreover, it is acknowledged that, CI originating or existing outside of the EU, but interconnected or having a potential direct effect on EU MS should also be considered.

Question

Should ECI be infrastructure that has a potentially serious cross-border impact with two or more MS, or three or more MS? Why?

6.2. Interdependencies

It is suggested that the progressive identification of all ECI in particular take into account interdependencies. Studies in interdependencies would contribute to assessing the potential impact of threats against specific CI and in particular to identify which MS would be affected in case of a major CI related incident.

Full consideration would be given to interdependencies within and between businesses, industry sectors, geographical jurisdictions and MS authorities in particular those enabled by Information and Communications Technologies (ICTs). The Commission, the MS and the owners/operators of critical infrastructures would work together to identify these interdependencies and apply appropriate strategies to reduce risk where possible.

Question

How can interdependencies be taken into account?

Do you know of any suitable methodologies for analysing interdependencies?

At what level should the identification of interdependencies take place – at EU and/or MS level?

6.3. Implementing steps for ECI

The Commission would suggest the following implementing steps for ECI:

(1) The Commission together with the MS draw up the specific criteria which would be used to identify ECI on a sector-specific basis;

(2) Progressive identification and verification on a sector-by-sector basis of ECI by MS and Commission. The decision on designating particular CI as ECI will be taken at the European level[1] due to the cross border nature of the infrastructure concerned.;

(3) MS and Commission analyse existing security gaps in relation to ECI on a sector-by-sector basis;

(4) MS and Commission agree on priority sectors/infrastructure for action, taking into account interdependencies;

(5) Where relevant, for each sector, the Commission and MS key stakeholders agree on proposals for minimum protection measures, which could include standards;

(6) Following the adoption of the proposals by the Council, these measures are then implemented;

(7) Regular monitoring is ensured by the MS and the Commission. Revisions (measures and identification of CI) are made when and where appropriate.

Questions

Is the list of steps concerning the implementation of the ECI acceptable?

How do you suggest the Commission and the MS designate together ECI - MS have expertise, Commission has overview of European interest? Should this be a legal decision?

Is there a need for an arbitration mechanism if a particular MS do not agree to designate an infrastructure under its jurisdiction as ECI?

Is there a need for verification of designations? Who should be responsible?

[1] With the exception of defence-related infrastructures.

Should MS be able to designate infrastructure in other MS or third countries as being critical for them? What should happen if a MS, a third country or an industry considers a piece of infrastructure in a MS to be critical for them?

What should happen if that MS then does not identify it? Is there a need for an appeals mechanism? If so what?

Should an operator have the possibility of appealing, if they do not agree with their designation or non-designation. If so, to whom?

What methodologies would need to be developed for setting priority sectors/infrastructure for action? Do suitable methodologies already exist that can be adapted to the European-level?

How can the Commission be involved in analysing the security gaps in relation to ECI?

7. NATIONAL CRITICAL INFRASTRUCTURES (NCI)

7.1. The NCI role in EPCIP

Many European companies operate across borders and as such are subject to differing obligations for NCI. It is therefore suggested in the interests of the MS and the EU as a whole that each MS protects its NCI under a common framework so that owners and operators throughout Europe would benefit from not being subject to a varied puzzle of frameworks resulting in a multitude of methodologies and additional costs. To that extent the Commission suggests that EPCIP – while focusing primarily on EU Critical Infrastructure - cannot leave out altogether National Critical Infrastructure. Nevertheless, three options could be envisaged:

a) NCI is fully integrated within EPCIP

b) NCI is outside the scope of EPCIP

c) MS may use parts of EPCIP at their own volition in relation to NCI, but are under no obligation to do so.

Question

The efficient protection of critical infrastructure in the European Union would seem to require the identification of both ECI and NCI. Do you agree that although EPCIP should focus on ECI, NCI cannot altogether be left out?

Which of these options do you feel is the most appropriate for EPCIP?

7.2. National CIP programmes

Based on a common EPCIP framework, MS could develop National CIP Programmes for its NCI. The MS would be able to apply more stringent measures than those provided for under EPCIP.

Question

Is it desirable that each MS adopts a National CIP Programme based on EPCIP?

7.3. Single overseeing body

The need for efficiency and coherency suggests the necessity of designation by each MS of a single overseeing body dealing with the overall implementation of EPCIP. Two options could be envisaged:

(a) A single CIP overseeing body;

(b) A national contact point with no authority, leaving it to the MS to organise themselves.

Such a body could coordinate, monitor and oversee the implementation of EPCIP within its jurisdiction and could serve as the main institutional contact point on CIP matters with the Commission, other MS and CIP owners and operators. This body could form the basis for national representation in expert groups dealing with CIP issues and could be connected to the Critical Infrastructure Warning Information Network (CIWIN). The National CIP Coordination Body (NCCB) could coordinate national CIP issues notwithstanding that other bodies or entities within a MS that may already be involved in CIP matters.

The progressive identification of NCI could be achieved by obliging infrastructure owners and operators to notify the NCCB about any relevant CIP related business activity.

The NCCB could be responsible for the legal decision on designating an infrastructure under its jurisdiction as a NCI. This information would remain at the sole disposal of the MS concerned.

Specific competences could include:

a) Coordination, monitoring and overseeing the overall implementation of EPCIP in a MS;

b) Serving as the main institutional contact point on CIP matters with:

   i. the Commission

   ii. other MS

   iii. CIP owners and operators

c) Participate in the designation of EU Critical Infrastructure (ECI);

d) Taking the legal decision on designating an infrastructure under its jurisdiction as a National Critical Infrastructure;

e) Serve as an authority of legal recourse for owners/operators who do not agree that their infrastructure is designated “critical infrastructure”;

f) Participate in the elaboration of the National Critical Infrastructure Protection Programme and the sector specific CIP programmes;

g) Identify interdependencies between specific CI sectors;

h) Contribute to sector-specific approaches to CIP through participation in expert groups. Owners and operators representatives could be invited in order to contribute to the discussions. Regular meetings could be held;

i) Supervise the process of drawing-up CI related contingency plans;

Questions

Do you agree that MS would alone be responsible for designating and managing NCI under a common EPCIP framework?

Is it desirable to designate a CIP coordination body within each MS having overall coordination responsibility for CIP related measures while respecting existing sector based responsibilities (civil aviation authorities, Seveso Directive etc.)?

Would the suggested competences of such a coordination body be appropriate? Are there others that are necessary?

7.4. Implementing steps for NCI

The Commission would suggest the following implementing steps for NCI:

(1) Using EPCIP, the MS draw up the specific criteria which would be used to identify NCI;

(2) Progressive identification and verification on a sector-by-sector basis of NCI by MS;

(3) MS analyse existing security gaps in relation to NCI on a sector-by-sector basis ;

(4) MS set-up priority sectors for action, taking into account interdependencies and EU level agreed priorities where relevant;

(5) Where relevant, for each sector, the MS agree minimum protection measures;

(6) MS are responsible for ensuring that the owners/operators under their jurisdiction carry out the necessary implementation measures;

(7) Regular monitoring is ensured by the MS. Revisions (measures and identification of CI) are made when and where appropriate.

Question

Is the list of steps concerning the implementation of the NCI appropriate? Are any steps superfluous? Should any steps be added?

8. ROLE OF CI OWNERS, OPERATORS AND USERS

8.1. Responsibilities of CI owners, operators and users

Designation as a CI suggests certain responsibilities for owners and operators. Four responsibilities could be envisaged for owners and operators designated as NCI or ECI:

(1) **Notification to the relevant MS CIP body of the fact that an infrastructure may be of a critical nature**;

(2) **Designation of a senior representative(s) to act as Security Liaison Officer (SLO) between the owner/operator and the relevant MS CIP authority**. The SLO would take part in the development of security and contingency plans. The SLO would be the main liaison officer with the relevant CIP sector body in the MS and where relevant with the law enforcement authorities;

(3) **Establishment, implementation and updating of an Operator Security Plan (OSP).** A suggested OSP template is attached in Annex 3.

(4) **Participation in the development of a contingency plan** relative to the CI with relevant MS civil protection and law enforcement authorities where requested.

The OSP could be submitted for approval to the relevant MS CIP sector authority under the overall supervision of the NCCB regardless if it is a NCI or ECI which would guarantee the consistency of security measures taken by specific owners and operators and the relevant sectors in general. In return owners and operators could be given relevant feedback and support as to relevant threats, development of best practices and where appropriate help in assessing interdependencies and vulnerabilities through the NCCB and where relevant by the Commission.

Each MS could set a time limit for the creation of the OSP by the owners and operators of NCI and ECI (in the case of ECI the Commission would also be involved) and could set administrative fines for situations when these deadlines are not respected.

It is suggested that the Operator Security Plan (OSP) would identify the owner's/operator's critical infrastructure assets and establish relevant security solutions for their protection. The OSP would describe the methods and procedure which are to be followed to ensure compliance with EPCIP, National CIP Programmes and relevant sector specific CIP programmes. The OSP could represent a vehicle for a bottom up approach in regulating CIP that gives stronger leeway (and also more responsibility) to the private sector.

In particular situations when it comes to certain infrastructure such as electricity grid networks and information networks it would be unrealistic (from a practical and financial point of view) to expect the owners and operators to provide equal levels of security to all their assets. In such cases, it is suggested that the owners and operators could, together with the relevant authorities identify the critical points (nodes) of a physical or information network on which security protective measures could be concentrated.

The OSP could contain security measures arranged around two headings:

- **permanent security measures**, which would identify indispensable security investment and means, which cannot be installed by the owner/operator at short notice. The owner/operator would maintain a standing alertness against potential threats, which would not disturb its regular economic, administrative and social activities.

- **graduated security measures**, which could be activated according to varying threat levels. The OSP would therefore foresee various security regimes adapted to possible threat levels existing in the MS where the infrastructure is located.

It is suggested that failure on behalf of a CI owner and operator to adhere to the obligation of developing an OSP, contribute to the development of contingency plans and designating an SLO could entail the possibility to impose a financial penalty.

Questions

Are the potential responsibilities for owners/operators of critical infrastructure acceptable in terms of increasing the security of critical infrastructure? What would be their likely cost?

Should owners and operators be obliged to notify the fact that their infrastructure may be of a critical nature?Do you think the OSP concept is useful? Why?

Are the suggested obligations proportional to the costs involved?

What rights could the CI owners and operators be given by the MS authorities and Commission?

8.2. Dialogue with CI owners, operators and users

EPCIP could engage the owners and operators in partnerships. The success of any protection programme depends on the cooperation and level of involvement that can be achieved with the owners and operators. Within the MS, the CIP owners and operators could be closely involved in CIP developments through regular contacts with the NCCB.

At EU level, forums could be created in order to facilitate exchanges of views on general and sector specific CIP issues. A common approach on private sector engagement on CIP related issues to bring together all stakeholders in the public and private sphere would provide the MS, Commission and the industry with an important platform through which to communicate on whichever new CIP issue arise. The owners, operators and users of CI could assist in the development of common guidelines, best practice standards and where relevant information sharing. Such dialogue would help shape future revisions of EPCIP.

Where relevant the Commission could encourage the creation of EU CIP related industry/business associations. The two ultimate objectives would be to ensure that European industry retains its competitiveness and that the security of EU citizens is enhanced.

Question

How should the dialogue with the owners, operators and users of CI be structured?

Who should represent the owners, operators and users in the public private dialogue?

9. EPCIP SUPPORTING MEASURES

9.1. The critical infrastructure warning information network (CIWIN)

The Commission has developed a number of rapid alert systems allowing for the concrete, coordinated and effective response in case of emergencies, including those of a terrorist origin. On 20 October 2004, the Commission announced the creation of a central network in the Commission ensuring rapid information flows between all Commission rapid alert systems and concerned Commission services (ARGUS).

The Commission is suggesting creating CIWIN which could stimulate the development of appropriate protection measures by facilitating an exchange of best practices in a secure manner as well as being a vehicle for transmission of immediate threats and alerts. The system would ensure that the right people have the right information at the right time.

The following three options are possible for the development of CIWIN:

(1) **CIWIN would be in the shape of a forum limited to the exchange of CIP ideas and best practices** in support of the CI owners and operators. Such a forum could take the form of a network of experts and an electronic platform for the exchange of relevant information in a secure environment. The Commission would play an important role in gathering and disseminating such information. This option would not provide the necessary rapid alerts on imminent threats. However there could be scope for the broadening of CIWIN in the future.

(2) **CIWIN would be a rapid alert system (RAS) linking MS with the Commission.** This option would increase the security of critical infrastructure by providing warnings limited to immediate threats and alerts. The objective here would be to facilitate a rapid exchange of information about potential threats to CI owners and operators. The RAS would not involve the sharing of long-term intelligence. It would be used for the rapid sharing of information on imminent threats to specific infrastructure.

(3) **CIWIN would be a multi-level communication/alert system composed of two distinct functions:** a) a rapid alert system (RAS) linking MS with the Commission and b) a forum for the exchange of CIP ideas and best practices in support of the CI owners and operators composed of a network of experts and an electronic data exchange platform.

Regardless of the option chosen, CIWIN would complement existing networks and due care taken to avoid duplication. In the long-term, CIWIN could be linked to all relevant CI owners and operators in each MS through for instance the NCCB. Alerts and best practices could be channelled through this body which would be the only service directly connected to the Commission and thereby to all other MS. MS would be able to utilize their existing information systems for the establishment of their national CIWIN capacity linking the

authorities to specific owners and operators. Importantly, these national networks could be used by the relevant MS CIP bodies and the owners and operators as a two way communication system.

A study will be launched to determine the scope and technical specifications necessary for CIWIN's future interface with the MS.

Questions

What form should the CIWIN network take in order to support the objectives of EPCIP?

Should CI owners and operators be connected to CIWIN?

9.2. Common methodologies

Different MS have different alert levels corresponding to different situations. At the present time there is no way of knowing whether, for example, a "high" in one MS, is the same as a "high" in another. This may make it difficult for trans-national companies to prioritise their expenditure on protection measures. It may be beneficial, therefore to attempt to harmonise or calibrate the different levels.

For every level of threat, there could be a level of preparedness whereby common security measures may be triggered in general and, where appropriate, the use of graduated security measures in particular. MS not wishing to deploy a certain measure would be able to address a specific threat by alternative security measures.

A common methodology of identifying and classifying threats, capabilities, risks, and vulnerabilities and drawing conclusions about the possibility, probability, and degree of severity posed by a threat to disrupt an infrastructure installation could be considered. This would include risk rating and prioritization in which risk events could be defined in terms of their probability of occurrence, impact, and relationship to other risk areas or processes.

Questions

To what extent is it desirable and feasible to harmonise or calibrate different alert levels?

Should there be a common methodology of identifying and classifying threats, capabilities, risks, and vulnerabilities and drawing conclusions about the possibility, probability, and degree of severity posed by a threat?

9.3. Funding

Following an initiative of the European Parliament (creation of a new budget line – pilot project « Fight against terrorism" – in the 2005 budget), the Commission took the decision on 15th September to allocate 7 Mio€ to finance a set of actions which will enhance European prevention, preparedness and response to terrorist attacks, including consequence management, critical infrastructure protection, terrorist financing, explosives and violent radicalisation. More than two thirds of this budget is consecrated to the preparation of the future European Programme for Critical Infrastructure protection, to the integration and development of capabilities required for the management of Crises of trans-national significance resulting from possible terrorist attacks and to emergency measures which may

be required to address a significant threat or occurrence of such an attack. It is expected that this funding will continue in 2006.

From 2007 to 2013 funding will be taken over by the Framework programme on Security and Safeguarding Liberties. This will include a Specific Programme on "Prevention, Preparedness and Consequence Management of Terrorism"; the Commission's proposal allocated an amount of € 137,4 million designed to identify the relevant needs and to develop common technical standards to protect critical infrastructure.

The programme will provide Community funding to projects presented by national, regional and local authorities for the protection of critical infrastructures. The programme focuses on identifying protection needs and at providing information in view of developing common standards, threat and risk assessments, in order to protect critical infrastructure, or develop specific contingency plans. The Commission would make use of its existing expertise or could help finance studies concerning interdependencies in specific sectors. It is then mainly the responsibility of the MS or the owners and operators to upgrade the security of their infrastructure according to the identified needs. The programme itself does not fund the upgrading of critical infrastructure protection. Loans from financial institutions could be used for upgrading the security of infrastructure in the MS according to the needs identified through the programme, and to implement common standards. The Commission would be willing to support sector based studies to assess financial impacts the upgrading of security of infrastructure may have on the industry.

The Commission is funding research projects in support of critical infrastructure protection in the Preparatory Action for Security Research[2] (2004-2006), and has planned more substantial activities in the area of security research in its proposal for a Decision of the Council and the European Parliament concerning the 7th EC Research Framework Programme (COM(2005)119 final)[3] and its proposal for a Council Decision concerning the Specific programme "Cooperation" implementing the Seventh Framework Programme (COM(2005)440 final). Targeted research which aims to provide practical strategies or tools for risk mitigation is of prime importance to securing EC's critical infrastructure in the medium to long-term. All Security Research, including in this area, will be submitted to ethical review to ensure compatibility with the Charter of Fundamental Rights. The demand for research will only increase as the number of infrastructure dependencies increase.

Questions

How would you estimate the cost and impact of the implementation of the measures put forward in this green paper for administrations and industry? Would you find it proportionate?

[2] The total sum of credits in the 2004 and 2005 budgets amounted to €30 million. For 2006, the Commission has proposed the sum of €24 million, which is being examined by the budget authority.

[3] The budget proposal of the Commission for security and space related research activities under the 7th RTD framework programme amounts to €570 million (COM(2005)119 final)

9.4. Evaluation and monitoring

Evaluation and monitoring of the implementation of EPCIP suggests a multi-level process which requires the involvement of all stakeholders:

- **at EU level, a peer evaluation mechanism could be established**, in which MS and the Commission would work together on assessing the overall level of implementation of EPCIP in each MS. Commission annual progress reports concerning the implementation of EPCIP could be prepared.

- **the Commission would report progress to MS and other institutions each calendar year** in a Commission staff working paper.

- **at MS level, the NCCB in each MS could monitor the overall EPCIP implementation under its jurisdiction ensuring the compliance with National CIP Programme(s) and sector specific CIP programmes,** to ensure that they are effectively implemented through yearly reports to Council and Commission.

EPCIP implementation would be a dynamic process, constantly evolving and evaluated both to keep pace with the changing world and to build on lessons learnt. Peer review evaluations and MS monitoring reports could be part of the instruments used to review EPCIP and suggest new measures to strengthen the protection of critical infrastructure.

Relevant information by the MS concerning ECI could be made available to the Commission for the development of common vulnerability assessments, consequence management plans, common standards for the protection of CI, prioritising research activities and, where necessary, regulation and harmonisation. Such information would be classified and kept strictly confidential.

The Commission could monitor various MS initiatives, including those that foresee financial consequences for owners and operators incapable of resuming essential services to citizens within a specified maximum timeframe.

Question

What type of evaluation mechanism would be needed for EPCIP? Would the above mentioned mechanism be sufficient?

The responses should be sent electronically by 15 January 2006 to the following e-mail address: **jls-epcip@cec.eu.int**. These will be kept confidential unless the responder explicitly states that they want it made public, in which case they will be placed on the Commission's internet site.

ANNEXES

ANNEX 1

CIP TERMS AND DEFINITIONS

This indicative list of definitions could be further built upon depending on the individual sectors for the purpose of identification and protection of Critical Infrastructure (CI).

Alert

Notification that a potential disaster situation will occur, exists or has occurred. Direction for recipient to stand by for possible escalation or activation of appropriate measures.

Critical infrastructure protection (CIP)

The ability to prepare for, protect against, mitigate, respond to, and recover from critical infrastructure disruptions or destruction.

Critical Information Infrastructure (CII):

ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.).

Critical Information Infrastructure Protection (CIIP)

The programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of critical information infrastructures in case of failures, attacks or accidents above a defined minimum level of services and aim at minimising the recovery time and damage.

CIIP should therefore be viewed as a cross-sector phenomenon rather than being limited to specific sectors. CIIP should be closely coordinated with Critical Infrastructure Protection from a holistic perspective.

Contingency plan

A plan used by a MS and critical infrastructure owner/operator on how to respond to a specific systems failure or disruption of essential service.

Contingency plans would typically include the development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental and public-assistance programs to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration as well as development of initiatives to mitigate the effects of future incidents.

Critical Information

Specific facts about a critical infrastructure asset, vitally needed to plan and act effectively so as to guarantee failure or cause unacceptable consequences for critical infrastructure installations.

Critical Infrastructure (CI)

Critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments.

There are three types of infrastructure assets:

- Public, private and governmental infrastructure assets and interdependent cyber & physical networks.
- Procedures and where relevant individuals that exert control over critical infrastructure functions.
- Objects having cultural or political significance as well as "soft targets" which include mass events (i.e. sports, leisure and cultural).

Essential service

Often applied to utilities (water, gas, electricity, etc.) it may also include standby power systems, environmental control systems or communication networks that if interrupted puts at risk public safety and confidence, threatens economic security, or impedes the continuity of a MS government and its services.

European critical infrastructure (ECI)

European critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets, which, if disrupted or destroyed would have a serious impact on the health, safety, security, economic or social well-being of two or more MS.

The definition of what constitutes an EU critical infrastructure is determined by its cross border effect which ascertains whether an incident could have a serious impact beyond two or more MS national territories. This is defined as the loss of a critical infrastructure element and is rated by the:

- extent of the geographic area which could be affected by the loss or unavailability of a critical infrastructure element beyond three or more Member State's national territories;
- effect of time (i.e. the fact that a for example a radiological cloud might, with time, cross a border);
- level of interdependency (i.e. electricity network failure in one MS effecting another);

Impact

Impacts are the total sum of the different effects of an incident. This needs to take into account at least the following qualitative and quantitative effects:

- *Scope* - The loss of a critical infrastructure element is rated by the extent of the geographic area which could be affected by its loss or unavailability - international, national, regional or local.

- *Severity* - The degree of the loss can be assessed as None, Minimal, Moderate or Major. Among the criteria which can be used to assess impact are:

  - Public (number of population affected, loss of life, medical illness, serious injury, evacuation);

  - Economic (GDP effect, significance of economic loss and/or degradation of products or services, interruption of transport or energy services, water or food shortages);

  - Environment (effect on the public and surrounding location);

  - Interdependency (between other critical infrastructure elements).

  - Political effects (confidence in the ability of government);

  - Psychological effects (may escalate otherwise minor events).
    both during and after the incident and at different spatial levels (e.g. local, regional, national and international)

- *Effects of time* - This criteria ascertains at what point the loss of an element could have a serious impact (i.e. immediate, 24-48 hours, one week, other).

Interdependency

Identified connections or lack thereof between and within infrastructure sectors with essential systems and assets.

Occurrence

The term “occurrence” in the CIP context is defined as an event (either human caused or by natural phenomena) that requires a serious emergency response to protect life or property or puts at risk public safety and confidence, seriously disrupts the economy, or impedes the continuity of a MS government and its services. Occurrences include negligence, accidents, deliberate acts of terrorism, computer hacking, criminal activity and malicious damage, major disasters, urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, storms, public health and medical emergencies and other occurrences requiring a major emergency response.

Operator Security Plan

The Operator Security Plan (OSP) identifies all of the operator's critical infrastructure assets and establishes relevant security solutions for their protection. The OSP describes the methods and procedures which are to be followed by the owner/operator.

Prevention

The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from an incident. Prevention involves efforts to identify threats, determine vulnerabilities and identify required resources.

Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and as appropriate specific law enforcement operations aimed at deterring, pre-empting, interdicting, or disrupting illegal activity, and apprehending potential perpetrators and bringing them to justice. Prevention involves the stopping of an incident before it happens with effective processes, guidelines, standards and certification. Seamless interactive systems, and comprehensive threat- and vulnerability analysis.

Prevention is a continuous process of ongoing actions to reduce exposure to, probability of, or potential loss from hazards.

Response

Activities that address the short-term direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at pre-empting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

Risk

The possibility of loss, damage or injury. The level of risk is a condition of two factors: (1) the value placed on the asset by its owner/operator and the impact of loss or change to the asset, and (2) the likelihood that a specific vulnerability will be exploited by a particular threat.

Threat

Any indication, circumstance, or event with the potential to disrupt or destroy critical infrastructure, or any element thereof. An all-hazards approach to threat includes accidents, natural hazards as well as deliberate attacks. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets.

Vulnerability

A characteristic of an element of the critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat.

ANNEX 2

INDICATIVE LIST OF CRITICAL INFRASTRUCTURE SECTORS

Sector		Product or service	
I	Energy	1	Oil and gas production, refining, treatment and storage, including pipelines
		2	Electricity generation
		3	Transmission of electricity, gas and oil
		4	Distribution of electricity, gas and oil
II	Information, Communication Technologies, ICT	5	Information system and network protection
		6	Instrumentation automation and control systems (SCADA etc.)
		7	Internet
		8	Provision of fixed telecommunications
		9	Provision of mobile telecommunications
		10	Radio communication and navigation
		11	Satellite communication
		12	Broadcasting
III	Water	13	Provision of drinking water
		14	Control of water quality
		15	Stemming and control of water quantity
IV	Food	16	Provision of food and safeguarding food safety and security
V	Health	17	Medical and hospital care
		18	Medicines, serums, vaccines and pharmaceuticals
		19	Bio-laboratories and bio-agents
VI	Financial	20	Payment services/payment structures (private)
		21	Government financial assignment
VII	Public & Legal Order and Safety	22	Maintaining public & legal order, safety and security
		23	Administration of justice and detention
VIII	Civil administration	24	Government functions
		25	Armed forces
		26	Civil administration services
		27	Emergency services
		28	Postal and courier services
IX	Transport	29	Road transport
		30	Rail transport
		31	Air traffic
		32	Inland waterways transport
		33	Ocean and short-sea shipping
X	Chemical and nuclear industry	34	Production and storage/processing of chemical and nuclear substances
		35	Pipelines of dangerous goods (chemical substances)
XI	Space and Research	36	Space
		37	Research

ANNEX 3

OPERATOR SECURITY PLAN

The possible contents of the OSP should include an introduction and a classified detail part (not accessible outside the relevant MS authorities). The classified part would begin with a presentation of the operator and describe the legal context of its CI activities. The OSP would then go on to presenting the details on the criticality of the infrastructure concerned, taking into consideration the operator's objectives and the Member State's interests. The critical points of the infrastructure would be identified and their security requirements presented. A risk analysis based on major threat scenarios, vulnerability of each critical point, and potential impact would be conducted. Based on this risk analysis, relevant protection measures should be foreseen.

Introduction)

Contains information concerning the pursued objectives and the main organisational and protection principles.

Detailed part *(classified)*

– **Presentation of the operator**

Contains a description of the operator's activities, organization and connections with the public authorities. The details of the operator's Security Liaison Office (SLO) are given.

– **Legal context**

The operator addresses the requirements of the National CIP Programme and the sector specific CIP programme where relevant.

– **Description of the criticality of the infrastructure**

The operator describes in detail the critical services/products he provides and how particular elements of the infrastructure come together to create an end-product. Details should be provided concerning:

- material elements;
- non-material elements (sensors, command, information systems);
- human elements (decision-maker, expert);
- access to information (databases, reference systems);
- dependence on other systems (energy, telecoms);
- specific procedures (organisation, management of malfunctions, etc.).

– **Formalisation of security requirements**

The operator identifies the critical points in the infrastructure, which could not be easily replaced and whose destruction or malfunctioning could significantly disrupt the operation of the activity or seriously endanger the safety of users, customers or employees or result in essential public needs not being satisfied. The security of these critical points is then addressed.

The owners, operators and users ('users' being defined as organizations that exploit and use the infrastructure for business and service provision purposes) of critical infrastructure would have to identify the critical points of their infrastructure, which would be deemed restricted areas. Access to restricted areas should be monitored in order to ensure than no unauthorised persons and vehicles enter such areas. Access would only be granted to security cleared personnel. The relevant background security checks (if deemed necessary by a MS CIP sector authority) should be carried out by the Member State in which the critical infrastructure is located.

– **Risk analysis and management**

The operator conducts and risk analysis concerning each critical point.

– **Security measures**

The operator presents the security measures arranged around two headings:

- Permanent security measures, which will identify indispensable security investment and means, which cannot be installed by the owner/operator in a hurry. The owner/operator will maintain a standing alertness against potential threats, which will not disturb its regular economic, administrative and social activities. 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 may be activated according to varying threat levels. The OSP will therefore foresee various security regimes adapted to possible threat levels existing in the Member State.

– **Presentation and application**

The operator will prepare detailed information sheets and instructions on how to react to various situations.

– **Monitoring and updating**

The operator sets out the relevant monitoring and updating mechanisms which will be used.