COUNCIL OF THE EUROPEAN UNION

Brussels, 18 December 2006 (19.12)
(OR. fr)

16933/06
ADD 1

Interinstitutional File:
2006/0276 (CNS)

PROCIV 273
JAI 725
COTER 64
ENER 323
TRANS 345
TELECOM 133
ATO 174
ECOFIN 472
ENV 713
SAN 270
CHIMIE 43
RECH 365
DENLEG 61
RELEX 929

COVER NOTE

from:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	15 December 2006
to:	Mr Javier SOLANA, Secretary-General/High Representative
Subject:	COMMISSION STAFF WORKING DOCUMENT Accompanying document to 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 SUMMARY OF THE IMPACT ASSESSMENT

Delegations will find attached Commission document SEC(2006) 1648.

Encl.: SEC(2006) 1648

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 12.12.2006
SEC(2006) 1648

COMMISSION STAFF WORKING DOCUMENT

Accompanying document to 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

SUMMARY OF THE IMPACT ASSESSMENT

{COM(2006) 787 final}
{SEC(2006) 1654}

SUMMARY OF THE IMPACT ASSESSMENT

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.

Critical infrastructure can be damaged, destroyed or disrupted through a variety of both manmade and natural occurrences. Any such disruptions or manipulations of critical infrastructure 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.

What is the problem?

The problem which needs to be addressed is the vulnerability of critical infrastructures in Europe and the ensuing vulnerability of the services they provide. The underlying problem is that a low level of protection of critical infrastructure in certain Member States has the potential to increase the vulnerability of other Member States.

Who is affected?

The problem potentially affects all inhabitants of the European Union, businesses, the Member State governments and the European Union as a whole. Effects can be both direct (e.g. casualties following a terrorist attack) and indirect (e.g. the disruption of certain services following the surfacing of problems with a particular infrastructure).

Why is EU level action urgently needed?

- A growing number of Member States are preparing their own approaches to critical infrastructure protection and are waiting for the Commission to put forward a general European CIP programme, so that they can take into account the common EU approach. Delaying the adoption of a common framework would increase the chance that various incompatible approaches to CIP would be developed by the Member States.

- Weak links have to be eliminated especially where transboundary effects came into play. The risk of one Member State suffering because another has failed to adequately protect infrastructure on their territory needs to be minimised.

- Additional costs for companies operating in more than one Member State resulting from differing security measures need to be minimised.

- Some infrastructure are becoming increasingly European, which means that a purely national approach is insufficient e.g. the energy pipelines and transmission network.

- Some of the work concerning the details of how to better protection critical infrastructure in Europe (especially on such issues as the identification of interdependencies) can reasonably be expected to take a long time. Such work should start as quickly as possible and needs to be based on a common approach.

- Stakeholder consultations have been ongoing since 2004 and have included three EU CIP Seminars, the adoption of a Green Paper, the holding of two informal CIP contact points meetings and numerous bilateral meetings with government and private sector representatives.

- Criminal and terrorist threats are not diminishing and there is an interest, and synergies, in Member States and the Commission cooperating to protect against them.

Objective

The general objective of a proposed policy on critical infrastructure protection would be to improve the protection of critical infrastructure in the EU.

The advantages and drawbacks of the four distinct policy options

A number of possible policy options have been identified with a view to achieving the above mentioned objective:

1. Refraining from addressing CIP issues at a European level. Under this option no horizontal actions would be undertaken at European level.

   The "no policy change" option does not present any clear strengths in terms of improving the protection of critical infrastructure in Europe. It does present however a number of disadvantages stemming from competition issues, greater costs for businesses, insufficient security. This approach has been disqualified by all Member States who generally see a need to address critical infrastructure protection from a European perspective.

2. The creation of a non-binding framework. Under this option a non-binding horizontal framework would be created, but the Member States would be free to decide whether they want to make use of it.

   The "non-binding framework" option possesses the clear advantage of creating a framework designed to build trust among all stakeholders. This advantage cannot however balance out the strong disadvantages stemming from this option including growing costs, competition issues and the heightened security risk. The issue of security is a key problem of this Option. A non-binding framework will not provide the needed basis to have all Member States implement sufficient protection measures for their critical infrastructure.

3. The creation of a light legislative framework. Under this option, a number of binding measures would be implemented at European level. The Member States would be subjected to certain general obligations, but strong emphasis would still be put on the exchange of best practices, dialogue and the building of trust at EU level.

   The "light legislative framework" option provides the best balance of advantages and disadvantages. This approach would safeguard competition, lower costs for businesses operating in more than one Member State and increase security in the European Union. These clear advantages would seem to outweigh the disadvantages associated with costs. Another possible disadvantage of this option stems from the

fact that it creates another regulatory framework in the EU. However, in the interest of security, this approach seems to be justified.

4. Full harmonization at EU level. Under this option, full harmonization measures would be proposed at EU level concerning the organization of CIP issues in the Member States as well as regarding the protection requirements relevant to the owners/operators of critical infrastructure.

   The "full harmonization" option creates several clear advantages and disadvantages. On the positive side, EU critical infrastructure would be protected to a high degree. On the downside, high costs would be involved and it would be difficult to build trust among stakeholders. Finally, this option has already been disqualified by the Member States, which want EPCIP to build on and complement their existing achievements. This approach could be contrary to the subsidiarity and proportionality principles and would most likely be rejected by all Member States.

The analysis of the four policy options mentioned above confirms that action at European level would have an added value and is indeed needed. Option 3 would seem to offer the biggest advantages.

However, taking into account the fact that EPCIP constitutes a completely new policy and that there is therefore a need for a step-by-step approach in the CIP field, the best practicable option would consist of a combination of options 2 and 3. The overall framework of EPCIP would thereby be addressed by a non-binding instrument, while a few key requirements concerning ECI would be introduced through binding measures.

Impacts of recommended policy consisting of binding and non-binding measures

The need for a comprehensive and consistent step-by-step approach to establishing EPCIP would merit a combination of binding and non-binding measures.

For each of the key elements, the impacts of binding and non-binding instruments are assessed[1]. Since EPCIP's general objective is to improve the protection of critical infrastructure in the EU, the positive impact on security of the key elements is weighed against the potential costs.

1. *Participation in CIP expert groups at EU level.* Building trust among all stakeholders involved in the CIP process is crucial for its long term success. Such CIP expert groups would have a very positive impact in terms of security. Costs would be limited as CIP expert groups would only be setup where needed and on a *pro bona* basis. As EU level expert groups would function on a voluntary basis, they should form part of the non-binding framework of EPCIP.

2. *Use of a secure CIP information sharing process.* The CIP information sharing process among relevant stakeholders requires a relationship of trust. Supporting a voluntary CIP information exchange cannot be done by way of binding measures as these would be counterproductive in terms of building trust and facilitating dialogue. The impact on security would of course be positive. Costs can be expected to remain

[1] Some elements can due to their nature only be addressed by non-binding measures, for example the setting up of expert groups. In these cases the assessment will be limited to the non-binding approach.

low as the measures remain non-binding and are relevant more for an introduction of a certain security oriented "state of mind".

3. *Identification and analysis 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. No binding measures can be imposed in this regard as the identification of interdependencies is part of a broader process which requires cooperation and coordination between several stakeholders. An estimation of costs cannot be made at this time as the process of identifying interdependencies is of an ongoing nature. EU funding could contribute to this process.

4. *Elaboration of National CIP Programmes.* While clearly the responsibility for protecting National Critical Infrastructure falls on the NCI owners/operators and on the Member States, there would also be a Community benefit in making sure that the issue of National Critical Infrastructure is being sufficiently addressed in each of the Member States. Although having clear security benefits, the introduction of a binding approach to National CIP Programmes may not be possible at first. Subsidiarity and the need for a step-by-step approach to EPCIP may justify the concentration of binding measures on ECI related issues. The use of a non-binding approach to National CIP Programmes may be justified. This approach would however have to be re-assessed once work progresses on the issue of ECI.

5. *Identification of national critical infrastructure by each Member State.* The identification of National Critical Infrastructure is a prerequisite for making sure that they are being adequately protected. The use of a binding approach concerning the identification of NCI would give stronger security benefits than a non-binding approach. Nevertheless, due to subsidiarity and the need to concentrate at first on ECI issues, the use of a non-binding approach to the identification of NCI may be justified. As the EU's experience in the CIP field grows, this approach may however have to be re-assessed.

6. *Nomination by each Member State of a CIP contact point.* There is a need for each Member State to designate a CIP contact point, who would have a general overview of CIP activities in the Member State and would coordinate CIP within the Member State and with other Member States, the Council and the Commission. Only a binding approach would guarantee that each Member State performs the necessary tasks. Non-binding measures could be mildly successful, but could in no way guarantee that each Member State would nominate a CIP Contact Point. A binding approach to CIP Contact Point designation would therefore be preferred.

7. *Identification and designation of European critical infrastructure.* The identification and designation of ECI is at the heart of EPCIP, as improving the protection of critical infrastructure can only occur once the relevant infrastructure have been identified. This process needs to be completed in a coordinated fashion and can only be successful when undertaken at EU level.

   Only a binding approach to the identification and designation of ECI can provide a high probability of success in terms of achieving EPCIP's objectives. Moreover, a binding approach in this regard would have two further positive consequences:

- transparency – if the identification and designation is subject to a legal procedure it is subject to scrutiny by Member States – and potentially by others, this way transparency is maximised,

- comparability – ensuring that there are common procedures and methods will mean that the ECI identified will be comparable, and will not be subject to potentially very different interpretations by Member States.

If a non-binding approach to this process would be used, the EU would be faced with a situation in which only certain European critical infrastructure having an EU importance would be identified. It is in the interest of the entire EU to eliminate such weak links.

8. *Conducting vulnerability, threat and risk assessments for ECI.* Each Member State should conduct a risk and threat assessment in relation to relevant ECI. Such assessments would be done in order to improve the protection of ECI. Due to this action's role in the entire process of strengthening the protection of ECI, the use of a binding instrument in this regard would be justified. Without making sure that all Member States conduct relevant assessments, the ECI owners/operators will not have sufficient information concerning potential threats and an EU level assessment of protection gaps could not be conducted.

9. *Obligations of European Critical Infrastructure.* In order to achieve the objective of improving the protection of ECI, three measures to be undertaken by the ECI owners/operators should be considered: the designation of a Security Liaison Officer and the elaboration of an operator security plan. The use of a binding instrument concerning these two obligations is justified as it would not be possible to achieve a coherent approach to the protection of ECI across the EU in any other way. If non-binding measures were used, only a certain number of ECI would comply. The possible costs involved would at least be counter weighed by increased security, which means more stability, predictability and an increase in consumer confidence for the business environment, thus resulting in an increase in business opportunities and investments.

Conclusion

The analysis of the specific impacts of the nine key measures suggests that a combination of binding and non-binding measures would be best suited to achieving the objectives of EPCIP while providing the best cost/benefit ratio. In terms of the nine key measures, five would be better placed in a non-binding framework, while four should be made obligatory:

(I) Non-binding measures:

a) participation in CIP expert groups at EU level;

b) use of a CIP information sharing process;

c) identification and analysis of interdependencies;

d) elaboration of national CIP programmes;

e) identification of national critical infrastructure;

(II) Binding measures:

a) nomination of CIP Contact Points;

b) identification and designation of European Critical Infrastructure;

c) conducting threat and risk assessments for ECI;

d) elaboration of Operator Security Plans; designation of Security Liaison Officers.

As a consequence, the recommended policy for the creation of EPCIP would consist of:

1. A general non-binding EPCIP framework set out in a Commission Communication.

2. A binding instrument dealing specifically with ECI (ECI Directive). This instrument would set out a common approach to the identification and designation of ECI of the assessment of the need to improve their protection.