COUNCIL OF THE EUROPEAN UNION

Brussels, 18 December 2006

16933/06 ADD 2

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 Impact Assessment

Delegations will find attached Commission document SEC(2006) 1654.

Encl.: SEC(2006) 1654

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 12.12.2006
SEC(2006) 1654

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

IMPACT ASSESSMENT

{COM(2006) 787 final}
{SEC(2006) 1648}

Table of contents

Impact assessment

The European Programme for Critical Infrastructure Protection

Executive summary

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.

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

The general objective of a proposed policy on critical infrastructure protection would be to improve the protection of critical infrastructure in the EU. A number of possible policy options have been identified with a view to achieving this objective:

1. Refraining from addressing CIP issues at a European level.
2. The creation of a non-binding framework.
3. The creation of a light legislative framework.
4. Full harmonization at EU level.

Following a careful analysis and due to the broad scope of the envisaged policy and the need for a step-by-step approach to CIP, it appeared that setting up EPCIP by a non-binding instrument such as a Communication, complemented by a restricted number of binding measures, offers the best cost/benefit ratio and best satisfies the underlying objective of improving the protection of critical infrastructure in Europe and thereby increasing the security of the European Union and its citizens.

Section 1: Procedural issues and consultation of interested parties

Organisation and timing

Reference number: 2006/JLS/045

Work on the European Programme on Critical Infrastructure Protection began in 2004 following the terrorist attacks in Madrid. Relevant work has been taken forward through the Critical Infrastructure Protection sub-group of the Interservice Group on the Internal Aspects of the Fight Against Terrorism. This CIP sub-group is chaired by DG JLS with participation from: DG TREN, DG MARKT, DG INFSO, DG ADMIN, DG ECFIN, DG ENTR, DG SANCO, DG RTD, DG ENV, JRC, DG REGIO, DG RELEX, DG BUDG, OLAF, SJ and SG.

Consultation and expertise

All relevant stakeholders have been consulted concerning the development of EPCIP. This has been done through:

- The EPCIP Green Paper adopted in on 17 November 2005 with the consultation period ending on 15 January 2006. 22 Member States provided official responses to the consultation. Around 100 private sector representatives also provided comments to the Green Paper. The responses were generally supportive of the idea of creating EPCIP. Summary reports concerning the responses received from the Member States and the private sector to the EPCIP Green Paper consultation are included in Annex 1 and 2.
- Three Critical Infrastructure Protection seminars hosted by the Commission (in June 2005, September 2005 and March 2006). All three seminars brought together representatives of the Member States. The private sector was invited to the seminars held in September 2005 and March 2006.
- Informal meetings of CIP Contact Points. The Commission hosted two meetings of the CIP Contact Points of the Member States (December 2005 and February 2006).
- Informal meetings with private sector representatives. Numerous informal meetings were held with representatives of particular private business as well as with industry associations.

Impact of the Green Paper responses on the EPCIP proposal

As a result of the responses received to the EPCIP Green Paper and of ongoing discussions with all stakeholders, the following issues have had a major impact in shaping the proposal for EPCIP:

- *Goal of EPCIP*. The goal of EPCIP has been changed to improving the protection of critical infrastructure in the EU. Previously, the proposed goal of EPCIP was to ensure that there are adequate and equal levels of protective security on critical infrastructure. Several stakeholders underlined in their responses to the EPCIP Green Paper that the setting of equal levels of protective security across all sectors would not only be extremely difficult to achieve, but could also be counterproductive in terms of increasing security overall as sector specificities would not be taken into account sufficiently.
- *Key principles*. The list of key principles has been expanded to include the "sector-by-sector approach". The remaining principles have also been modified.
- *Common EPCIP framework*. It is explicitly acknowledged that the common EPCIP framework must be of a general nature and should contain only the most important

provisions needed to facilitate future work. Specific work along with further regulatory activities (where relevant) will be taken forward on a sectoral basis.

- *ECI and NCI.* The approach to ECI and NCI has been clearly separated, by introducing a common approach to ECI at EU level and leaving the introduction of similar approaches for NCI to the Member States, where necessary supported by the Commission. .
- *Implementing steps for ECI and NCI.* The implementing steps have been amended in order to take account of the varying role the EU may play in relation to ECI as compared to NCI. A structured system of implementation has been proposed consisting of three Work Streams (the first of a strategic/horizontal nature, the second concerning ECI, the third concerning NCI).
- *Single overseeing body.* The Member States remain free to establish administrative structures as they see fit in order to deal with CIP. EPCIP would only require that each Member State designate a CIP Contact Point who would coordinate CIP issues within the Member State and with other Member States, the Council and the Commission.
- *National CIP Programmes.* EPCIP would only encourage each Member State to develop a National CIP Programme based on a certain set of recommended elements.
- *Identification of NCI.* It has been clarified that the identification of NCI would remain in the hands of the Member States.
- *Identification of ECI.* A set of procedures for the identification and designation of ECI has been put forward.
- *Owners/operators of critical infrastructure.* Their obligations and rights have been clarified.
- *Confidentiality and information exchange.* Due to the very big importance attributed to this issue by stakeholders, confidentiality and the exchange of CIP related information has been specifically address.

Section 2: Problem definition

What is the issue or problem that may require action?

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 existence and operation of for example - telecommunication and energy networks, banking and transport systems, health services, the provision of safe drinking water and food - is crucial to the functioning of the European Union and its Member States. The destruction or disruption of infrastructure providing key services could entail *inter alia* 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 in a multitude of ways including deliberate acts of terrorism, natural disasters, negligence, accidents or computer hacking, criminal activity and malicious behaviour. 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 (MS), their citizens and the European Union. The recent terrorist attacks in Madrid and London have highlighted the risk of terrorist attacks against infrastructure in Europe.

The critical infrastructure present in the European Union is currently subjected to a varying puzzle of protective measures and obligations. Some Member States have already identified their national critical infrastructure and have imposed strong protection measures. Several other Member States are not as advanced however. In certain cases, there has been no concerted effort to even identify the critical infrastructure present under a particular jurisdiction.

Despite the fact that some work has been undertaken at national level in order to deal with national critical infrastructure, very little has been done in terms of studying the interdependencies existing between critical infrastructure in various sectors as well as the interdependencies existing between infrastructure located in different Member States. No effort has been done to identify those critical infrastructures which if disrupted or destroyed could have a significant effect on the functioning of the Community as a whole or a number of Member States. It is clear however that such critical infrastructure exist.

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.

It is clear, that the security of critical infrastructure is only as strong as its weakest link. In other words, even if one Member States imposes very high security standards in relation to a particular cross-border infrastructure, that infrastructure and the services it provides will still be vulnerable if another Member State does not impose adequate protection measures on its side.

It is also evident that in today's interconnected world, infrastructure physically located in a single Member State may offer services to other Member States or may have an impact on the provision of services in other Member States. In the case of such infrastructure, it is equally important to provide this particular infrastructure with a sufficient level of security so that the security of other Member States, who are dependent on the service that infrastructure provides or may be influenced by that infrastructure, is ensured. The interdependencies existing between the various sectors create a situation where a particular event may have a cascading effect on other sectors

and areas of life, which are not immediately and obviously interconnected. For example, a terrorist attack on a power plant may disrupt the power supplies over a large area and may influence the provision of other services including medical services due to the lack of electricity. Interdependencies exist within and between businesses, industry sectors, geographical jurisdictions and MS authorities in particular those enabled by Information and Communications Technologies (ICTs).

Many European companies operate across borders and as such are subject to differing obligations concerning critical infrastructure. On the purely economic side, the existence of a multitude of protection levels and standards across EU Member States increases costs for businesses, which have to incur duplicating security investments depending on the jurisdictions under which they operate.

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. The basic principle of coexistence or sharing of a common space implies however that no co-owner of that common space should allow that any harm be caused, deliberately or not, to their neighbours.

The problem in general

The issue at hand which requires action is the vulnerability of critical infrastructures in Europe and the ensuing vulnerability of the services they provide. This applies to all critical infrastructures in Europe regardless of whether they can be considered as having EU or national importance.

Taking into account the principles of subsidiarity and proportionality, EU level action should concentrate on those critical infrastructures having an EU importance. With this in mind, EPCIP will develop into a process leading over time to an assessment of vulnerabilities of particular CI sectors and the preparation of proposals on how to best address these vulnerabilities. These key activities and especially the development of specific protection measures will concentrate on European critical infrastructure, with the Member States however being encouraged to adopt similar approaches concerning their national critical infrastructure.

What are the underlying drivers of the problem?

The vulnerability of critical infrastructure in the European Union is caused by:

- Certain owners/operators of critical infrastructure may not be implementing sufficient protection measures (possibly because they are not aware of potential risks or they do not want to over-invest is security and put themselves in a competitive disadvantage vis-à-vis other businesses)
- Certain Member States do not possess detailed and systemised knowledge about the existence of critical infrastructure under their jurisdiction.
- Certain Member States have not established a national approach to strengthening the protection of critical infrastructure under their jurisdiction
- No systematic effort has been made to identify interdependencies existing between sectors and between critical infrastructure existing in various Member States.

Who is affected, in what ways, and to what extent?

The problem potentially affects all European citizens, inhabitants of the European Union, 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).

- *Citizens*. The existence of vulnerable infrastructure affects EU citizens by way of the potential loss of lives, the destruction of private property and the disruption of services.
- *Business*. The existence of vulnerable infrastructure affects EU businesses by way of the potential destruction of property and the disruption of services/shipments businesses rely on. EU businesses are very much interdependent (both geographically and in terms of sectors), so a disruption/destruction of a single critical infrastructure may have detrimental effects on a number of associated businesses. It is moreover worth mentioning, that competition among businesses creates a situation in which businesses are less likely to invest in sufficient security if their competitors aren't investing either.
- *Governments*. Governments are affected by the existence of vulnerable infrastructure as they too are dependent on services provided by such infrastructure. The potential disruption/destruction of critical infrastructure may wane public confidence in acting governments.

The costs for owners/operators of critical infrastructure should a disruption or destruction of infrastructure occur

Risks to critical infrastructure industries are becoming more and more interdependent as the economic, technological, and social processes of globalization intensify. The challenge of ensuring reliable operations has increased because operations both within and among companies have become increasingly interdependent. Elements of infrastructure in particular have become so interdependent that the destabilization of one is likely to have severe consequences for others.

As the scale and reach of technological systems have increased, the potential economic and social damage of failures has increased as well. The sources of such major disruptions lie in technical and managerial failures as well as natural disasters or terrorist attacks. Economic and social activities are becoming more and more interdependent as well, so that the actions taken by one organization will affect others.

In this context, the incentives for any single organization to invest in prevention, response, and recovery are blunted. Without an EU approach to understanding interdependencies and security externalities, determining the source of disruptions and quantifying the risk of such disruptions are difficult. Private decision-makers will have neither adequate information nor adequate motivation to undertake investments that are more than justifiable from the standpoint of the system as a whole.

Strategies to protect critical infrastructure are not viable unless they are politically and economically sustainable. Sustainability may be enhanced by a deliberate policy of seeking win-win options that promise public and private benefits beyond vulnerability reduction. Public relations, reputation, and the possibility of tort liability may motivate some firms to invest.

Understanding the motives, constraints, and capabilities of potential attackers may inform decisions regarding investments in prevention, response, and recovery.

A market economy routinely accounts for improved efficiency, because shareholders are always looking for the best return on investment in the short term. However, vulnerability may be assessed only after it has been exposed by active study or system failure. In addition, organizations are most likely to account for vulnerabilities that are linked to their own core activities.

Accountability for and accounting of vulnerabilities distant from core business activities are relatively uncommon, particularly when the perceived probabilities of occurrence are very low. Although economic incentives drive the accounting of core-business vulnerabilities, legal, organizational, and political dynamics drive the response to vulnerabilities that lie outside the core business concerns of any single firm or industry.

The cumulative impact of terrorist attacks and natural disasters has raised the bar on corporate governance. Owners/operators are increasingly under heightened scrutiny to identify vulnerabilities and prepare flexible disaster recovery plans to protect corporate as well as personal assets as well as prepare for, and manage catastrophic emergencies that can have a crippling effect on their business.

Protecting employees, revenue, and assets are all components of a well thought out plan aimed at minimizing loss and liability. A critical infrastructure owner/operator's failure to identify its exposures and evaluate the impact of potential losses could be disruptive to the continuity of its business leaving its executives open to severe legal actions and public criticism. While owners/operators of critical infrastructure may have good reasons not to make public disclosures regarding security breaches, one would expect their incentives to measure the costs of such incidents internally to be strong.

Without accurate cost data (how would critical infrastructure owners/operators assess the risks they face, make rational decisions about how much to spend on information security, or evaluate the effectiveness of security efforts etc.) it is very difficult to quantify the costs ensuing from potential terrorist attacks, natural disasters or other major occurrences. These costs will depend on the sector in which the disrupted/destroyed infrastructure operates, its size, interdependencies etc. What we can be sure of is that depending on the nature of the threat, a number of direct and indirect costs will affect not only the entity which was the object of the attack/occurrence, but also its business partners, employees and the wider public.

Given the uncertainties in measuring costs, risks, and the effectiveness of security efforts, we cannot make simple statements like the following: a company that expects to lose x euros per year to cyber attacks, natural disasters or terrorism will generally spend y euros to mitigate those losses.

In the case of a terrorist attack against a particular infrastructure asset, the relevant costs could be incurred in five areas:

1. The owners/operators that were the target of the attack. Direct impacts would include casualties, physical damage, and loss of production capacity. Indirect consequences could include the resignation of staff, loss of business.

2. Other actors located in the physical proximity of the target. Direct impacts could include casualties and physical damage. Indirect consequences could include resignation of staff and the loss of business.
3. Associated actors. Costs would be incurred for example by the business partners of the targeted owners/operators who would no longer be able to supply a specific product or service.
4. All other actors including the broader public. This will entail a fall in business and consumer confidence.
5. The cost will also be related to the government's emergency response and reconstruction efforts

The macroeconomic costs stemming from a terrorist attack continue to grow as businesses become more interdependent. Unfortunately, terrorist attacks themselves are increasingly inexpensive to conduct. To illustrate the disproportions existing between these costs, it is worth recalling the costs of carrying out some recent terrorist attacks.

The November 1998 twin truck bombings of the U.S. embassies in Kenya and Tanzania was estimated to cost less than $50,000. The September 11, 2001 attack cost an estimated $500,000. 231 people died in the two embassy bombings while almost 3,000 died during September 11, 2001. The cost of reconstruction of the U.S. embassies was a fraction of the $2 trillion estimated reconstruction cost and losses caused by Sept. 11, 2001.

The cost of the terrorist attack in Istanbul in November 2003 was estimated at less than $40,000. Four suicide truck bombings hit four different targets, killing 62 people. The attack reversed the country's slow economic recovery and caused a capital outflow by Western investors.

The Madrid bombings killed 191 people and cost as little as $10,000. The London and Sharm el Sheikh attacks in 2005 killed 55 and 88 people respectively and cost roughly the same or less, yet their potential socio-economic impact (potential cost of lost business, reconstruction, insurance and security) is much higher. In the case of the London and Madrid bombings, the reduction to the Spanish and UK's gross domestic product appears to have been negligible.

Effective action to combat terrorism will generate significant benefits for the global economy, preventing losses from reduced trade flows and investment undermining economic growth. Since international goods and financial markets transmit terrorism's costs well beyond the country where acts occur and terrorist groups operate across borders, any economy's actions to curb terrorist activities should produce global and regional benefits. Similarly, failure to counter terrorism will produce costs for all economies and populations. When consumers feel less safe, it changes their spending patterns. Businesses will change their investment and employment plans. Lack of confidence negatively impacts growth.

A sustainable critical infrastructure policy must account for tradeoffs that exist not only at company level between efficiency and vulnerability but also for institutions and the incentives potentially affecting that trade-off. Ultimately, policy must

- structure incentive systems for investment that enhance prevention of, response to, and recovery from the most likely and damaging attacks;

- ensure adequately robust internal operations of private firms, including greater system reliability for their services;
- limit imposed costs on firms to guarantee the competitiveness of the economy; and
- do all of the above in a manner that can be sustained by a public with a short memory that may tire of the high costs and consumer inconvenience that policies aimed at making critical industries less vulnerable may entail.

Cost is a significant issue when considering security of critical infrastructure in the EU. A lot of money is already spent by government agencies (e.g. police, border guards) and by commercial organisations (e.g. for security of premises). Increasing the security against terrorism will cost even more money. However budgets of both governments and commercial organisations are getting increasingly tight, and money for new security measures will be hard to find. In some ways, cost is a key driver and may be more significant than technology in terms of the level of security that can be provided within the EU[1].

Security costs money in two basic ways: cost of security equipment and cost of security staff. Some security equipment can save in staff costs. For example, automatic processing of CCTV images can reduce the number of staff required to monitor CCTV, thus saving on staff costs, while at the same time increasing security effectiveness. However, most new security equipment and procedures to increase effectiveness will require increased spending on security.

There are some significant differences between the costing philosophy for measures to fight *crime* (i.e. criminal acts for monetary gain) and for measures to fight *terrorism* (i.e. criminal acts to cause destruction and fear). Acts of crime are much more frequent than acts of terrorism, and counter crime measures effectively pay for themselves in terms of reduced financial losses. In fact commercial organisations may allow a measure of loss due to fraud or theft because measures to give 100% protection against fraud or theft are seen as not cost effective.

The problem with security against terrorism is that if an attack does not happen, the money could be regarded as having been wasted – although it could be instead be regarded as a form of insurance. However, if the same measures could protect both against terrorism and against more conventional crime, then the savings against crime will effectively pay (wholly or partially) for the security.

Some security costs can effectively be paid for by the end user by legislation which requires the service providers (e.g. transport company, utility) to provide a certain level of security. Thus, for example:

a) Transport security may be paid for by the traveller through increased fares
b) Goods security may be paid for by the sender/receiver through increased freight charges
c) Energy/telecoms/water security may be paid for by the customer through higher bills
d) Computer and data network security may be paid for by the customer through increased hardware/software costs, higher charges for sending data and higher rentals for connections/services.

[1] ESSRT Project funded by the European Commission under the PASR 2004 Programme (Thales Research and Technology; International Institute for Strategic Studies; Crisis Management Initiative; Thales e-Security).

If the cost increase due to extra security is below the rate of inflation, it might be easier to get it accepted. However, security legislation and consequent cost increases might push some business away from the EU to less security conscious nations.

Some security costs will have to be paid for out of taxation, e.g. border surveillance, law enforcement staff, armed response units on standby, security of government buildings and networks.

The difficulty with the economics of protection against terrorism is that there is no way of being fully sure that security measures are going to be effective. Millions of Euros might be spent on advanced security measures and an attack with very costly consequences still happens. It will be difficult to know if the security measures adopted had any real effect. Some clues might be given if an attack about to happen was prevented by the security measures. However it will be virtually impossible to quantify the deterrent effect of any security measures, i.e. whether terrorists would have tried an attack if those measures were not in place.

Another thing to consider is the difficulty of calculating the cost of national security -- and in particular of identifying the part of security costs that may be said to be counter-terrorism. A nation's security is paid for partly out of the defence budget, for which a global figure is usually given, but in most countries is very hard to break this down into its component parts. However, security is also paid for out of a range of other budgets: those of interior ministries, transport ministries, justice ministries, intelligence agencies, co-ordinating bodies, health service, local government bodies of all kinds, as well as private companies and individuals. This makes it virtually impossible to quantify security costs for each country, and to compare one country with another. For example, what proportion of a policeman's salary is attributed to national security/counter-terrorism?

An example of an indicative assessment of who is likely to pay for individual security measures directly and indirectly can be outlined as follows. This data is provided purely as an example of what types of security measures may be needed in order to improve the protection of critical infrastructure in Europe and the potential costs involved. Detailed impact assessments will accompany proposals for specific protection measures on a CIP sector-by-sector basis which may be developed where relevant. Cost issues will limit what can be achieved on European security, and spending must be prioritised wisely according to probability and impact of potential threats.

Security solution	Paid for by
Person access control	1. Boarding transport (e.g. aircraft, train) – *Paid for by transport companies and passed on within transport fares*
Person scanning	2. Crossing border – *Paid for within transport companies and passed on within transport fares (air/sea border), or by government from taxation (land border)*
Luggage scanning	3. Entering protected building or site – *Paid for by building/site user*
Vehicle access control	1. Boarding ship/train – *Paid for by transport companies and passed on within transport charges*
Goods integrity control	*2.* Crossing air/sea border - *Paid for within transport companies and passed on within transport fares*
Vehicle/ container/ goods scanning	3. Crossing land border *Paid for by government from taxation*
	4. Entering protected building or site – *Paid for by building/site user, but passed on to customers by users who are commercial organisations*
Perimeter protection	*Paid for by building/site user, but passed on to customers by users who are commercial organisations*
Land border surveillance	*Paid for by government from taxation*
Remote surveillance	1. Public area – *Paid for by area user, but passed on to customers by users who are commercial organisations* *2.* Public roads - *Paid for by government from taxation* 3. Other transport network – *Paid for by transport companies and passed on within transport charges* 4. Energy supply network – *Paid for by energy users*
Water quality checking	*Paid for by water companies and passed on in water charges*
General intelligence	*Paid for by government from taxation*
Ship and port protection	*Paid for within shipping and port companies/authorities and passed on within transport charges*
Maritime border protection	*Paid for by government from taxation*
Airspace protection	*Paid for by government from taxation*
CBR release detection	1. Public areas - *Paid for by users of the area, but passed on to customers by users who are commercial organisations* 2. Public events – *Paid for by government but passed on to event organisers and thence to event attendees*
EMP protection	1. Equipment - *Paid for in equipment costs* 2. Networks – *Paid for by network owners but passed on to customers*
Data and data network protection	*1.* Equipment and network within an organisation/agency - *Paid for by that organisation/agency* 2. Network between organisations/agencies – *Paid for by arrangement between the organisations/agencies served*

How would the problem evolve, all things being equal?

The problem would evolve taking into account the following:

- Member States would continue to address CIP issues individually
- A certain number of sectoral initiatives would appear at European level

If the problem would continue evolving without horizontal actions at EU level, no broader CIP coordination would exist. Consequently, there would be a strong risk that various incompatible sectoral approaches would be developed.

At national level, the EU Member States would continue to address CIP issues at their own pace. Certain Member States would continue to strengthen their CIP initiatives, while others would not pay much attention to the issue assessing their potential risk as low. Differences in protection measures among the Member States would mean that, especially for certain interdependent infrastructure, vulnerability would be quite high.

Businesses would refrain from investing in security issues as the existence of a multitude of standards and obligations would decrease their competitiveness.

Ultimately, the security of European citizens would suffer as a result.

Does the EU have the right to act?

Although several sectoral legal bases for critical infrastructure protection exist (e.g. in the transport and energy sectors), the Treaty does not specifically address CIP issues in a horizontal fashion. The Treaty establishing the European Community identifies nevertheless in Article 2 a number of objectives, whose attainment could be facilitated by strengthening the protection of critical infrastructure in Europe:

- To promote a harmonious, balanced and sustainable development of economic activities
- To promote a high degree of competitiveness
- To promote a high level of protection and improvement of the quality of the environment
- To promote the raising of the standard of living and quality of life
- To promote solidarity among Member States.

An EU policy on critical infrastructure protection would have to involve a number of sectors (in which varying forms of Community competence exist). Moreover, each of these sectors would have to deal with critical infrastructure protection by way of an all-hazards approach (involving both manmade and natural threats).

At present no act of the Community deals with the establishment or security aspects of a common framework for critical infrastructure protection in the EU.

The EU right to act has been acknowledged by the Council, which requested the Commission, to develop a programme to improve the protection of critical infrastructure in Europe.

The European Council of June 2004 asked for the preparation of 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 infrastructure.

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 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 by June 2006. The Conclusions state that "(…) the Council considers that action at EU level will add value by supporting and complementing Member States' activities, while respecting the principle of subsidiarity".

The subsidiarity principle is satisfied as the measures being undertaken through this proposal cannot be achieved by any single EU Member State and must therefore be addressed at EU level. Although it is the responsibility of each Member State to protect the critical infrastructure present under its jurisdiction, it is crucial for the security of the European Union to make sure that the most important infrastructure having an impact on two or more Member States or on a single Member State if the critical infrastructure is situated in another Member State are protected to a satisfying degree and that particular Member States are not made vulnerable because of the existence of lower security standards in other Member States.

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 that there is an interest, and potentially synergies, in Member States and the Commission cooperating to protect against them.

Section 3: Objectives

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

The specific and operational objectives needed in order for the general objective to be achieved are:

- Ensure that owners/operators of critical infrastructure implement adequate protection measures
    - Make sure that owners/operators of European Critical Infrastructure conduct sufficient risk assessments and prepare operator security plans
    - Make sure that owners/operators have access to best practices in the field of CIP
    - Ensure that all owners/operators of European Critical Infrastructure are subject to similar general requirements concerning critical infrastructure protection. These general requirements would not address the issue of specific protection measures, but would rather introduce a common approach on the steps to be taken and issues to be addressed by the owners/operators in order to improve the security of European critical infrastructure.
    - Ensure that owners/operators of European Critical Infrastructure are subjected to similar specific requirements concerning CIP within their particular sectors of activity so that competition within the internal market is not distorted. 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.
- Ensure that Member States identify and address critical infrastructure under their jurisdiction, and especially critical infrastructure which if disrupted or destroyed could have an effect on other Member States or the entire EU.
    - Encourage the Member States to create national CIP programmes
    - Participate in the identification and designation of particular infrastructure as national and/or European critical infrastructure
- Ensure EU level coordination and cooperation concerning the protection of critical infrastructure
    - Create a CIP contact group representing all Member States
    - Agree on common definitions
    - Exchange best practices
    - Designate critical infrastructure which could be of importance to the entire EU, to two or more Member States or to a single Member State if the critical infrastructure is situated in another Member State.
    - Identify interdependencies

- Ensure the security of all sensitive CIP data

Consistency with other EU policies

A proposal to create a European Programme for Critical Infrastructure Protection is consistent with other EU policies. In particular, several other sectoral policies, including transport and energy, are already taking forward work at a sectoral level concerning CIP. These sectoral policies rely to a certain extent on the creation of a horizontal programme which would make sure that consistent approaches to the issue are developed.

Section 4: Policy options

- Option 1: refrain from addressing CIP issues at a European level. Under this option no horizontal actions would be undertaken at European level and the Member States would be left to address the issue individually. This approach has been disqualified by all Member States who generally see a need to address the issue from a European perspective.
- Option 2: the creation of a non-binding framework. Under this option a non-binding horizontal framework would be created at European level, but the Member States would be free to decide whether they want to make use of it.
- Option 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 use of a Directive as the preferred legal instrument in this regard, would allow the Commission to make key issues obligatory for the Member States, but would give them the necessary freedom to adapt these obligations to their legal systems and CIP traditions.

  The Directive would respect national competences of the Member State and existing Community competences. Moreover, the sectoral competences of Commission services would be respected and relevant services would be expected to take forward sector specific work on critical infrastructure protection. The Directive would address such issues as:

  1. Set the objective of EPCIP and provide common general definitions
  2. Set the scope of EPCIP (all-hazards approach with a terrorism priority)
  3. Set out a list of critical infrastructure sectors relevant for EPCIP and a procedure for its amendment
  4. Set out how EPCIP would be implemented through the use of three work streams (the first on strategic issues, the second on European Critical Infrastructure, the third on National Critical Infrastructure)
  5. Oblige the Member States to designate CIP Contact Points who would coordinate CIP issues within each Member State and would participate in the EPCIP implementation work streams
  6. Oblige the Member States to elaborate National Critical Infrastructure Protection Programmes and to identify critical infrastructure under their jurisdiction
  7. Set out the procedure for the designation of European Critical Infrastructure
  8. Set out the procedure for developing specific protection measures for European Critical Infrastructure if such are required
  9. Set out the responsibilities of the owners/operators of critical infrastructure, in particular the designation of a Security Liaison Officer and the elaboration of an Operator Security Plan
  10. Set out the main rights of the owners/operators of critical infrastructure and the support available to them
  11. Provide a framework for the exchange of sensitive information and trust building measures.
  12. Set out an evaluation and monitoring mechanism.

- Option 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. This approach may be contrary to the subsidiarity and proportionality principles and would be rejected by all Member States.

Apart from the four distinct options listed above, a combination of options 2 and 3 could be used to setup EPCIP. Under such an approach, the overall EPCIP framework and supporting measures would be addressed by way of a non-binding instrument. A number of core issues, in particular concerning ECI, would however be subject to a binding approach. The assessment of this approach will be performed in section 7.

Section 5: Analysis of impacts of general policy

The impact of particular policy options on specific issues is measured below as a function of the magnitude of the impact and its likelihood. The magnitude of each impact should be viewed as the level of influence a particular policy option would have on specific issues falling within the economic, environmental and social context. The likelihood of an impact is the probability that this impact will occur.

Table of symbols (distinguishes "-" for costs and "+" for benefits	
Small magnitude	- / +
Medium magnitude	-- / ++
Significant magnitude	- - - / +++
Low likelihood	√
Medium likelihood	√√
High likelihood	√√√
No impact	0

Option 1: refrain from addressing CIP issues at a European level.

Economic impacts

- *Costs for businesses.* If nothing was to be done at EU level concerning Critical Infrastructure Protection the owners/operators of critical infrastructure would be subjected to varying approaches and protection requirements depending on the Member State in which they operate. As a consequence businesses would have to invest in varying protection measures in order to comply with obligations imposed by various Member States. Although it is likely that most (if not all) Member States will implement their own approaches to CIP resulting in increased costs for all owners/operators of CI (who will have to upgrade their protection measures in order to comply with national obligations), the greatest costs would be borne by businesses operating in more than one Member State. There would be a high risk that costs would increase disproportionately for such businesses, as they would have to comply with different CIP obligations in each of the Member States in which they operate. This trend would likely increase if nothing was done at EU level. Moreover, the existence of several different CIP regulatory environments in the EU would increase a feeling of insecurity among investors, consumers and other stakeholders which could lead to less investor and consumer confidence in the long term (i.e. the industry benefits from a secure environment, consumer and customer trust, etc.).
    - Magnitude of the negative impact on the costs for businesses operating in a single MS: -
        - Likelihood: √√√
    - Magnitude of the negative impact on the costs for businesses operating in more than one MS: - - -
        - Likelihood: √√√

- *Costs for authorities.* In order to implement any sort of CIP policy, Member State authorities must incur certain administrative costs in order to deal with CIP issues. These costs are associated with the need to create administrative structures dealing with CIP, hiring specialists etc. The likelihood of Option 1 having an impact on public authorities would be high, as most Member States see the need to address CIP issues. The magnitude of the impact would be medium.
    - Magnitude of the negative impact on the costs for authorities: - -
        - Likelihood: √√√
- *Negative impact on competition.* Competition may be affected as each Member State will impose different security obligations on businesses. Depending on the Member State, some companies will therefore have to invest more in security while others less. This would mean that businesses operating in certain Member States would be subjected to different obligations (and associated costs) despite the fact that they operate in similar or identical sectors. Moreover, the introduction of varying security standards in the EU Member States may constitute a significant barrier to entry into particular markets, especially for SMEs. The likelihood of this impact occurring would be high. The magnitude of the impact would also be high.
    - Magnitude of the negative impact on competition: - - -
        - Likelihood: √√√
- *Innovation and research.* Innovation and research is needed in order to improve the protection of critical infrastructure in Europe. This can include the development of improved risk assessment methodologies or even the development of new protection technologies. The EU is already promoting research and innovation in this area by way of such instruments as the Pilot Project – Terrorism (1st call for proposals concerning CIP was published in January 2006) and the Preparatory Action for Security Research. These as well as other initiatives relevant for CIP will continue. Impacts would therefore be limited in this regard. Option 1 would most likely not have a big effect on the stimulation of research activities. It would also be unlikely to promote greater resource efficiency as the existence of numerous approaches to CIP in the Member States would make the setting of priorities difficult.
    - Magnitude of the impact on the stimulation of research activities: +
        - Likelihood: √
    - Magnitude of the impact on promoting greater resource efficiency in relation to research: +
        - Likelihood: √

Environmental impacts

Positive impact in terms of reducing environmental risks. The implementation of some form of CIP policy in each Member State would help reduce the likelihood or scale of environmental risks (including the risk of fire, explosions, breakdowns, accidents and accidental emissions). Nevertheless, the lack of coordination and of a common approach to the protection of key infrastructure in Europe would mean that the likelihood of Option 1 having an impact on the prevention of certain risks and consequences would be low. The magnitude of the impact (if it

occurred) would be medium as certain vulnerabilities, especially concerning cross-border infrastructure, could not be protected against sufficiently through Option 1.

- Magnitude of the impact on reducing the likelihood or scale of environmental risks: ++
  - Likelihood: √

Social impacts

- *Increasing security in the EU.* The implementation of CIP policies in the Member States would help increase the security of CI in Europe and thereby of the entire EU. As there would be no common approach/obligation to implementing CIP policies, some Member States would most likely remain more advanced than others. Consequently, the general level of protection of critical infrastructure would most likely be insufficient (system is only as strong as its weakest link). The lack of a common approach to the protection of critical infrastructure having a European importance would also be counter productive in terms of decreasing vulnerability. The likelihood of Option 1 having an impact on EU security is high. The magnitude of the impact however on increasing security would be low.
  - Magnitude of the impact on increasing EU security: +
    - Likelihood: √√√
- *Stakeholder involvement*. Various stakeholders including businesses, associations, standards authorities and public authorities need to be involved at all level (national and EU) in the development of CIP policies. Under Option 1, the involvement of stakeholders in the development and implementation of CIP policies across the Member States would be varied. In some Member States this involvement would be high, in others lower. Only a limited dialogue would take place at EU level. The likelihood of Option 1 having an impact on stakeholder participation is low. The magnitude of the impact of option 1 in this regard would also be low.
  - Magnitude of the impact on stakeholder involvement: +
    - Likelihood: √
- *Administrative setup*. The implementation of a CIP policy requires the adaptation of public authorities to dealing with CI related tasks. The implementation of Option 1 would mean that Member States would be completely free to address CIP issues as they see fit. Those Member States which have not yet started to deal with CIP issues, would of course need to adapt their administrative setup to a greater degree than those Member States which are already advanced in the CIP area. In any case, depending on the approach adopted, most Member States would have to make certain modifications to their administrative setup in order to cope with the new responsibilities. The likelihood of Option 1 having an impact on public administration is medium. The magnitude is also medium.
  - Magnitude of the negative impact on public authorities due to the necessity to adapt the administrative setup: - -
    - Likelihood: √√

- *Positive impact on employment and labour markets.* Employment and labour markets would generally remain unaffected by the adoption of Option 1.
    - Magnitude of the impact on employment and labour markets: 0
        - Likelihood: 0
- *Building trust among stakeholders.* Building trust among all stakeholders involved in the CIP process is crucial for its long term success. Trust must be built among all stakeholders at both national and EU level. Option 1 would not facilitate any significant trust building at EU level. At national level, trust building would depend entirely on the approach adopted by each MS.
    - Magnitude of the impact on building trust among stakeholders: +
        - Likelihood: √
- *Improved protection of national critical infrastructure.* The adoption of Option 1 would imply that each Member State would concentrate on improving the protection of its own critical infrastructure, which would undoubtedly result in higher levels of security. Nevertheless, it must be kept in mind that most national critical infrastructure do not operate in a vacuum – they can still be influenced by infrastructure existing in other Member States or from outside the EU (by way of various interdependencies). Consequently, Option 1 would be likely to improve the protection of national critical infrastructure, but the magnitude of the improvement would only be low.
    - Magnitude of the impact on improving the protection of national CI: +
        - Likelihood: √√
- *Improved protection of European critical infrastructure.* The adoption of Option 1 would not foresee the possibility of identifying European critical infrastructure and would not facilitate improving the protection of CI's (in a coherent and coordinated fashion) having a European importance. Due to the lack of any coordinated approach to the identification and protection of European critical infrastructure, their vulnerability would increase.
    - Magnitude of the impact on improving the protection of European CI: +
        - Likelihood: √
- *Improving the exchange of best practices.* The exchange of best practices is a key element of strengthening CIP in Europe. The adoption of Option 1 would be unlikely to improve such exchanges, and in particular of making them available to all EU Member States. Some bilateral/multilateral cooperation schemes are most likely already taking place and would continue.
    - Magnitude of the impact on improving the exchange of best practices: +
        - Likelihood: √
- *Identification of interdependencies.* The identification of interdependencies is crucial in order to assess how various critical infrastructures interact and to identify potential vulnerabilities. By adopting Option 1, no coordinated effort concerning the identification of interdependencies would take place apart from existing and future research activities.
    - Magnitude of the impact on the identification of interdependencies: +

- Likelihood: √

Option 2: the creation of a non-binding framework

The creation of a non-binding framework would most likely have a better impact on improving the protection of critical infrastructure in Europe than Option 1. Option 2 would create a basic framework for cooperation at EU level, which could facilitate the exchange of best practices. Nevertheless, the Member States would still be free to decide as to the level of their participation in CIP activities, which could prevent certain states from taking the necessary measures in the CIP field (due for example to the costs involved). Infrastructure which could have an impact on more than one Member States as well as cross-border infrastructure would therefore not be protected to a satisfactory extent.

Economic impacts

- *Costs for businesses.* If a non-binding framework was created at EU level concerning Critical Infrastructure Protection the owners/operators of critical infrastructure would still be subjected to varying approaches and protection requirements depending on the Member State in which they operate (as under Option 1). In the short to medium term, the magnitude of the impacts as well as the likelihood would be the same as under Option 1 for both businesses operating in a single Member State and in more than one Member State. In the long term, as Member States increasingly discuss and cooperate on CIP issues, which could lead to the voluntary adoption of similar standards, the magnitude of the negative impact for businesses operating in more than one Member State could fall to medium. As there remains a certain amount of uncertainty whether such cooperation/coordination will actually occur to a satisfactory degree, the likelihood that costs for businesses would fall in the long term as compares to the short-medium term would be medium.
    - Magnitude of the negative impact on the costs for businesses operating in a single MS: -
        - Likelihood: √√√
    - Magnitude of the negative impact on the costs for businesses operating in more than one MS:
        - In the short to medium term: - - -
        - In the long term: - -
        - Likelihood:
            - In the short to medium term: √√√
            - In the long term: √√
- *Costs for authorities.* The creation of a non-binding framework should have a more positive effect than Option 1 on enticing the Member States to improve the protection of their critical infrastructure in a cooperative fashion. As the framework would be non-binding, the actual results may nevertheless be smaller than expected. In terms of costs for the authorities, the adoption of Option 2 would have a similar impact as Option 1 (medium). The likelihood of Option 2 having an impact would however be low as costs would not be directly associated with the implementation of the common framework, but would rather stem from national approaches to CIP already being implemented.

- Magnitude of the negative impact on the costs for authorities: - -
    - Likelihood: √

- *Negative impact on competition.* The consequences of adopting Option 2 would most likely be similar to Option 1. Nevertheless, Option 2 could lead to greater cooperation and coordination among the Member States. As a consequence, it may be possible to adopt similar protection measures at least in certain Member States or sectors. The likelihood therefore of having competition suffer within the internal market would drop to <u>medium</u> as compared to Option 1. The magnitude would remain <u>high</u>.
    - Magnitude of the impact on competition: - - -
        - Likelihood: √√
- *Innovation and research.* Option 2 would have a more positive impact on innovation and research than Option 1 as the Member States would cooperate more closely through the non-binding framework. Due to the existence of a common framework and the possibility of having similar protection measures, Option 2 would be likely (medium) to stimulate research activities. The magnitude of the impact would remain low nevertheless. Option 2 would be more likely to promote greater resource efficiency than Option 1, as the existence of a common CIP framework would help Member States agree on priorities. The magnitude of the impact would remain low however.
    - Magnitude of the impact on the stimulation of research activities: +
        - Likelihood: √√
    - Magnitude of the impact on promoting greater resource efficiency in relation to research: +
        - Likelihood: √√

<u>*Environmental impacts*</u>

Positive impact in terms of reducing environmental risks. The implementation of some form of CIP policy in each Member State would help reduce the likelihood or scale of environmental risks (including the risk of fire, explosions, breakdowns, accidents and accidental emissions). The existence of a light coordination system and of a basic common approach to the protection of key infrastructure in Europe under Option 2 would mean that the likelihood of this Option having an impact on the prevention of certain risks and consequences would be medium. The magnitude of the impact (if it occurred) would be medium (similar to Option 1).

- Magnitude of the impact on reducing the likelihood or scale of environmental risks: ++
    - Likelihood: √√

<u>*Social impacts*</u>

- *Increasing security in the EU.* Option 2 would have similar impact as Option 1 in terms of helping increase the security of critical infrastructure in Europe and thereby of the entire EU. This option envisages that would only be a non-binding framework concerning CIP with no obligations concerning the implementation CIP policies. Consequently, some Member States would most likely remain more advanced than others. The general level of protection of

critical infrastructure would therefore most likely be insufficient (the system is only as strong as its weakest point). The likelihood of Option 2 having an impact on the security of critical infrastructure is high. The magnitude of the impact however on increasing security would be low.

- Magnitude of the impact on increasing EU security: +
  - Likelihood: √√√

- *Stakeholder involvement*. Option 2 could potentially have a better effect on stakeholder involvement than Option 1, especially at European level. The involvement of stakeholders in the development and implementation of CIP policies across the Member States would remain varied. In some Member States this involvement would be high, in others lower. Option 2 could nevertheless provide a basic system of dialogue at EU level with relevant stakeholders. The likelihood of Option 2 having an impact on stakeholder participation is nevertheless low. The magnitude of the impact of option 1 in this regard would be medium.
  - Magnitude of the impact on stakeholder involvement: ++
    - Likelihood: √
- *Administrative setup*. The implementation of a CIP policy requires the adaptation of public authorities to dealing with CI related tasks. The implementation of Option 2 would mean that despite the existence of a non-binding framework, Member States would be free to address CIP issues as they see fit. Those Member States which have not yet started to deal with CIP issues would of course need to adapt their administrative setup to a bigger degree than those Member States which area already advanced in the CIP area. In any case, depending on the approach adopted, most Member States would have to make certain modifications to their structures in order to cope with the new responsibilities. The likelihood of Option 2 having an impact on public administration is medium. The magnitude is also medium.
  - Magnitude of the negative impact on public authorities due to the necessity to adapt the administrative setup : - -
    - Likelihood: √√
- *Positive impact on employment and labour markets*. Employment and labour markets would generally remain unaffected by the adoption of Option 2.
  - Magnitude of the impact on employment and labour markets: 0
    - Likelihood: 0
- *Building trust among stakeholders*. Building trust among all stakeholders involved in the CIP process is crucial for its long term success. Trust must be built among all stakeholders at both national and EU level. Option 2 would go a long way in terms of building trust, especially at EU level (stakeholders would gradually be involved in discussions concerning CIP issues). At national level, the non-binding framework could be used as a basis to start regular discussions with stakeholders, which over time, would help build trust among those involved. Nevertheless, at national level, trust building would depend entirely on the approach adopted by each MS.
  - Magnitude of the impact on building trust among stakeholders: +++

- Likelihood: √√

- *Improved protection of national critical infrastructure.* The adoption of Option 2 would imply that each Member State would concentrate on improving the protection of its own critical infrastructure, which would undoubtedly result in higher levels of security. Thanks to the creation of a non-binding framework under Option 2, it would nevertheless be possible to take more into account interdependencies and the broader international scene when it comes to CIP. Consequently, Option 2 would be likely to improve the protection of national critical infrastructure, but the magnitude of the improvement would only be medium.
    - Magnitude of the impact on improving the protection of national CI: ++
        - Likelihood: √√
- *Improved protection of European critical infrastructure.* Option 2 would foresee the possibility of identifying European critical infrastructure and cooperating on their protection. Option 2 would therefore have a more positive effect on the protection of European critical infrastructure than Option 1. The nature of the non-binding framework would mean nevertheless, that full cooperation may not be possible between the Member States in this regard (Member State may not want their infrastructure designated as European CI due to the costs involved etc).
    - Magnitude of the impact on improving the protection of European CI: ++
        - Likelihood: √√
- *Improving the exchange of best practices.* The exchange of best practices is a key element of strengthening CIP in Europe. The adoption of Option 2 would facilitate such cooperation. The magnitude of the positive impact could reach a high level as stakeholders would increasingly cooperate and have an interest in exchanging experiences and best practices under the voluntary framework. The likelihood would nevertheless remain low (as under Option 1) as it remains uncertain whether such exchanges would actually take place.
    - Magnitude of the impact on improving the exchange of best practices: +++
        - Likelihood: √
- *Identification of interdependencies.* The identification of interdependencies is crucial in order to assess how various critical infrastructures interact and to identify potential vulnerabilities. Option 2, would facilitate the identification of interdependencies by way of setting priorities, providing funding, facilitating the exchange of information.
    - Magnitude of the impact on the identification of interdependencies: ++
        - Likelihood: √√

<u>Option 3: the creation of a light legislative framework.</u>

The creation of a light legislative framework would most likely have a better impact on improving the protection of critical infrastructure in Europe than Option 2. A number of basic legal obligations of a horizontal nature would be put on the Member States and the owners/operators of critical infrastructure with a view to improving the protection of critical infrastructure. At the same time, the framework would be light enough to encourage dialogue and the building of trust between CIP stakeholders and could therefore have a positive effect on

future developments related to EPCIP. The strong side of this approach would be that all Member States would have to make an effort to improve the protection of critical infrastructure and would be able to do so by building on their existing systems. Even those Member States which are currently least prepared in the CIP field, would have to implement certain measures so as to increase the security of their critical infrastructure and by doing so increase the security of the entire EU.

Option 3 would be more likely to improve the situation of the private sector as more predictability and similarity concerning CIP measures among the Member States could be expected. Consequently, the owners/operators would be subjected to similar requirements in each of the Member States, which would be particularly beneficial for cross-border infrastructure.

In general terms, Option 3 would create the overall framework on how to address CIP issues from a European perspective and would put in place a limited number of mainly procedural obligations intended to facilitate the process of improving the protection of critical infrastructure. Under this option, specific protection measures would be developed at a later stage following a process elaborated in the framework, which would guarantee compatibility between national approaches.

Economic impacts

- *Costs for businesses.* If a light binding framework was created at EU level concerning Critical Infrastructure Protection the owners/operators of critical infrastructure would be subjected to similar approaches and to common minimum protection requirements in each of the Member State in which they operate. As a consequence businesses would have to invest in similar basic protection measures in order to comply with obligations imposed by the Member States. Businesses operating in more than one Member State would particularly benefit from this situation, as they would have to comply with similar CIP obligations in each of the Member States in which they operate. The magnitude of the impacts would be similar for both businesses operating in a single Member States and in more than one Member State. The likelihood of having an impact on costs for businesses operating in a single MS would remain high. The likelihood would be high that the costs for businesses operating in more than one MS would fall (as compared to Options 1 and 2) as these businesses would be able to take advantage of economies of scale. Despite the differences mentioned above, all infrastructure designated as national or European critical infrastructure would be subjected to at least two cost-incurring obligations: the designation of a Security Liaison Officer and the elaboration of an Operator Security Plan. It is not possible to quantify these costs as they will depend on the sector concerned and the infrastructure itself. It is safe to say however, that the costs stemming from these obligations should be relatively low as:
    - Infrastructures likely to be designated as national or European critical infrastructure most likely already have security officers. Consequently, the obligations imposed under the EPCIP framework would amount to giving an already existing security officer some additional tasks
    - The vast majority if not all of the infrastructure likely to be designated as national or European critical infrastructure already prepare business continuity plans. Such plans would be very similar in nature to the proposed Operator Security Plans.

  In other words, although a number of potential critical infrastructure already possess functions similar to SLOs and OSPs, the adoption of Option 3 would create an obligation to this effect on all infrastructure designated as national or European critical infrastructure. The

designation of SLOs and the creation of OSPs would not in itself be an objective of EPCIP under Option 3. It would be a means of achieving the overall objective of EPCIP, that is, to increase the security of critical infrastructure in Europe. It should also be underlined that although specifically consulted on these options during the EPCIP Green Paper consultation, none of the responses provided concrete figures or raised specific concerns as to the costs that these obligations could entail.

Other obligations which could cause additional costs (for e.g. concerning new protection measures etc.) would be developed as needed on a sector-by-sector basis and could be quantified then. It is worth mentioning nevertheless, that several sectors are already well prepared to cope with a number of different risks. In many cases therefore, the implementation of EPCIP will not imply big additional costs.

The costs for businesses mentioned above would be counter-weighed by a number of rights bestowed upon the owners/operators of national or European critical infrastructure. These could include access to best practices, access to EU CIP funding, participation in the development of specific measures under EPCIP.

Moreover, 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. Finally, as a consequence, potential new entrants will benefit as they will be faced with a foreseeable legal environment across the 25 Member States.

- Magnitude of the negative impact on the costs for businesses operating in a single MS: -
  - Likelihood: √√√
- Magnitude of the negative impact on the costs for businesses operating in more than one MS: -
  - Likelihood: √√√

- *Costs for authorities.* In order to implement any sort of CIP policy, Member State authorities must incur certain administrative costs in order to deal with CIP issues. The likelihood of Option 3 having a direct impact in this regard is medium (all Member States would have to have the necessary administrative structures in order to implement the common framework; several Member States however already have relevant structures in place). The magnitude of the impact of Option 3 would be medium as costs would not be directly associated with the implementation of the common framework, but would rather stem from national approaches to CIP already being implemented. The designation of CIP Contact Points should also not be viewed as an additional cost, as a vast majority of Member States (23) have already designated such contact points. The costs for administrations resulting from the adoption of the light binding framework could stem from:
  - The obligation to designate CIP Contact Points (as mentioned above, most Member States have already done so)
  - The obligation for each Member State to identify critical infrastructure under their jurisdiction (several Member States have already done this or are in the process). It would be difficult to quantify these costs as they depend on the approach adopted by

each Member State (whether it is the relevant authorities who identify the CI or is there an obligation on owners/operators to inform the relevant authorities about potential criticality), its size and the definition of what constitutes a national critical infrastructure.

- The obligation for each Member State to elaborate a National CIP Programme. Once again, several Member States already prepare such programmes. The process would nevertheless fall within the regular administrative activities of public authorities in a Member State.

Even, if certain administrative costs would prove to be necessary for the public authorities, these costs could legitimately be expected to be far outweighed by the benefits gained from increased security. These benefits, although not quantifiable, would touch upon the business environment, public confidence etc.

- Magnitude of the negative impact on the costs for authorities: - -
  - Likelihood: √√

- *Negative impact on competition.* Competition within the internal market is less likely to suffer if similar minimum protection requirements concerning critical infrastructure are implemented in each Member State. If security requirements are similar in all Member States, businesses will have to make similar investments. As a consequence, it will be unlikely that businesses in certain Member States will have to invest less due to security reasons. Of course, certain Member States may nevertheless decide to implement security obligations which go further than the minimum measures imposed by the common framework. The likelihood that competition would suffer as result of a light binding framework being adopted would be low. The magnitude of the impact would also be low.
  - Magnitude of the impact on competition: -
    - Likelihood: √

- *Innovation and research.* Innovation and research is needed in order to improve the protection of critical infrastructure in Europe. This can include the development of improved risk assessment methodologies or even the development of new protection technologies. The EU is already promoting research and innovation in this area by way of such instruments as the Pilot Project – Terrorism (1st call for proposals concerning CIP was published in January 2006) and the Preparatory Action for Security Research. These as well as other initiatives relevant for CIP will continue. Impacts would therefore be limited in this regard. Due to the existence of a common framework and the possibility to agree on research priorities, Option 3 would be likely (high) to stimulate research activities. The magnitude of the impact would be medium as stakeholders would be more likely to invest in CIP if there was a common approach to the issue and agreed minimum levels of protection among the Member States. Option 3 would be more likely (high) to promote greater resource efficiency than Options 1 and 2, as the existence of a common binding CIP framework would help Member States agree on priorities. The magnitude of the impact would be medium.
  - Magnitude of the impact on the stimulation of research activities: ++
    - Likelihood: √√√

- Magnitude of the impact on promoting greater resource efficiency in relation to research: ++
    - Likelihood: √√√

Environmental impacts

Positive impact in terms of reducing environmental risks. The implementation of a common binding CIP framework in each Member State would help reduce the likelihood or scale of environmental risks (including the risk of fire, explosions, breakdowns, accidents and accidental emissions). The existence of a coordination system and of a basic binding common approach to the protection of key infrastructure in Europe under Option 3 would mean that the likelihood of this Option having an impact on the prevention of certain risks and consequences would be high. The magnitude of the impact (if it occurred) would be high as various risks could be avoided due to increased cooperation built on the common framework (e.g. breakdowns of interdependent infrastructure located in different Member States).

- Magnitude of the impact on reducing the likelihood or scale of environmental risks: +++
    - Likelihood: √√√

Social impacts

- *Increasing security in the EU.* The implementation of CIP policies in the Member States would help decrease security risks concerning CI and increase the security of the EU. As there would be a binding CIP framework in the EU, the Member States would share a minimum level of security concerning their critical infrastructure which would be high enough to limit associated risks. Despite the existence of minimum protection measures, the Member States could still implement higher measures than those required by the common framework. Consequently, the general level of protection of critical infrastructure would most likely be sufficient, which would help safeguard the security of the EU and its citizens. The likelihood of Option 3 having an impact on the security of the EU is high. The magnitude of the impact on increasing security would also be high.
    - Magnitude of the impact on increasing EU security: +++
        - Likelihood: √√√
- *Stakeholder involvement*. The involvement of stakeholders in the development and implementation of CIP policies across the Member States would be similar as the common binding framework would envisage stakeholder participation in the development and implementation of CIP measures. At EU level, stakeholder involvement would be guaranteed through the binding framework. The existence of a binding framework would moreover mean that all parties would be interested in participating in relevant CIP discussions (the results of the discussions could form the basis for future obligations). The fact that the framework would be light and that a step-by-step approach would be taken would further encourage dialogue and participation. The light binding framework envisaged under Option 3 would foresee the active involvement of Member State authorities, Commission services, owners/operators or critical infrastructure and standardisation bodies in the development of EPCIP. The likelihood of Option 3 having an impact on stakeholder participation is high. The magnitude of the impact of option 1 in this regard would be high.

- Magnitude of the impact on stakeholder involvement: +++
  - Likelihood: √√√

- *Administrative setup.* The implementation of a CIP policy requires the adaptation of public authorities to dealing with CI related tasks. The implementation of Option 3 would mean that Member States would have to address CIP issues taking due regard to the common binding CIP framework. Those Member States which have not yet started to deal with CIP issues would of course need to adapt their administrative setup more than those Member States which are already advanced in the CIP area. In any case, depending on the approach adopted, most Member States would have to implement certain modifications to their structures in order to cope with the new responsibilities. The likelihood of Option 3 having an impact on public administration is medium. The magnitude is also medium.
  - Magnitude of the negative impact on public authorities due to the necessity to adapt the administrative setup : - -
    - Likelihood: √√

- *Positive impact on employment and labour markets.* Employment and labour markets could be affected by the adoption of Option 3. Increasing demand for security technologies and CIP research, as well as the implementation of certain CIP requirements may create new jobs. Moreover, the adoption of Option 3 could contribute to the creation of new market segments associated with security. On the other, hand most companies likely to be designated as critical infrastructure already fulfil similar obligations and have the necessary personnel to do it (business continuity plans are prepared; security officers exist). The magnitude of the positive impact on the labour market would therefore be low. The likelihood of its occurrence would also be relatively low.
  - Magnitude of the impact on employment and labour markets: +
    - Likelihood: √

- *Building trust among stakeholders.* Building trust among all stakeholders involved in the CIP process is crucial for its long term success. Trust must be built among all stakeholders at both national and EU level. Option 3 could have a positive effect on building trust among stakeholders at national and EU level (stakeholders would gradually be involved in discussions concerning CIP issues). Public-private dialogue and in consequence the involvement of various stakeholders in CIP discussions at EU level, would be foreseen by the framework. The fact that CIP measures would be developed gradually and based on a sector-by-sector approach would mean that trust could be built over time. It is worth mentioning as well that in several sectors, relevant expert groups already exist, where sufficient levels of trust have already been achieved to share relevant information. Such expert group would be used to build EPCIP.
  - Magnitude of the impact on building trust among stakeholders: +++
    - Likelihood: √√

- *Improved protection of national critical infrastructure.* The adoption of Option 3 would imply that each Member State would continue working on improving the protection of its own critical infrastructure, while taking into account interdependencies and the broader cross-

border context. As a result, each Member State could take into account in its CIP process vulnerabilities stemming from the fact that infrastructure are interconnected. Consequently, Option 3 would be likely to improve the protection of national critical infrastructure, and the magnitude of the improvement would be high.

- Magnitude of the impact on improving the protection of national CI: +++
  - Likelihood: √√

- *Improved protection of European critical infrastructure.* Option 3 would provide a framework for the identification and protection of European critical infrastructure. The framework would foresee the identification of European CI and relevant protection measures on a sector by sector basis. Due to the fact that work would on identifying and protecting European CI would be taken forward on a step-by-step basis with the involvement of all stakeholders and through dialogue, Option 3 provides an ideal mix of voluntary and obligatory measures in the interest of increasing the protection of European CI.
  - Magnitude of the impact on improving the protection of European CI: +++
    - Likelihood: √√
- *Improving the exchange of best practices.* The exchange of best practices is a key element of strengthening CIP in Europe. The adoption of Option 3 would facilitate such cooperation by way of cooperation between Member States and other stakeholders in forums created for CIP purposes. The Commission would play a key role in this area in terms of gathering best practices and making them available to those Member States which require such assistance.
  - Magnitude of the impact on improving the exchange of best practices: +++
    - Likelihood: √√√
- *Identification of interdependencies.* The identification of interdependencies is crucial in order to assess how various critical infrastructures interact and to identify potential vulnerabilities. Option 3, would facilitate the identification of interdependencies by way of setting priorities, providing funding, facilitating the exchange of information (like Option 2). The magnitude of the impact would therefore be high. The likelihood would be medium.
  - Magnitude of the impact on the identification of interdependencies: +++
    - Likelihood: √√

Option 4: full harmonization at EU level

The creation of a fully harmonized CIP system in the Member States would have a very strong effect on increasing the physical security of critical infrastructure in Europe, but would most likely be counter-productive in terms of building trust and dialogue among stakeholders. Consequently, the long-term development of EPCIP could be put at risk. On the economic side, the owners/operators of critical infrastructure would be subjected to identical requirements in all Member States which would significantly decrease their operational costs. This option has already been disqualified by most Member States and other stakeholders.

Economic impacts

- *Costs for businesses.* If full harmonization was attempted at EU level concerning Critical Infrastructure Protection the owners/operators of critical infrastructure would be subjected to

identical approaches and protection requirements in each of the Member State in which they operate. As a consequence businesses would have to invest in identical basic protection measures in order to comply with obligations imposed by the Member States. Businesses operating in more than one Member State would particularly benefit from this situation, as they would have to comply with identical CIP obligations in each of the Member States in which they operate. The magnitude of the impacts would be similar for both businesses operating in a single Member States and in more than one Member State. The likelihood of having an impact on costs for businesses operating in a single MS would remain high. The likelihood that Option 4 would have an impact on businesses operating in more than one Member State (costs would fall as compared to Options 1 and 2) would be high (such businesses would be able to take full advantage of economies of scale).

  - Magnitude of the negative impact on the costs for businesses operating in a single MS: -
    - Likelihood: √√√
  - Magnitude of the negative impact on the costs for businesses operating in more than one MS: -
    - Likelihood: √√√

- *Costs for authorities.* In order to implement any sort of CIP policy, Member State authorities must incur certain administrative costs in order to deal with CIP issues. The likelihood of Option 4 having a direct impact in this regard is high as all Member States would have to have the necessary administrative structures in order to implement the harmonized approach (those Member States already have CIP structures in place would have to reform them in order to abide by the harmonized approach). Option 4 would moreover entail additional administrative costs associated with strict compliance monitoring. The magnitude of the impact of Option 4 would be high as costs would stem directly from the implementation of the harmonized approach, which would supplant existing national initiatives.
  - Magnitude of the negative impact on the costs for authorities: - - -
    - Likelihood: √√√
- *Negative impact on competition.* Competition within the internal market is less likely to suffer if identical protection requirements concerning critical infrastructure are implemented in each Member State. If security requirements are identical in all Member States, businesses will have to make identical investments. As a consequence, the risk of varying levels of investment in security will be avoided. The likelihood that competition would suffer as a result of the harmonized approach to CIP being adopted would be low. The magnitude of the impact would also be low.
  - Magnitude of the negative impact on competition: -
    - Likelihood: √
- *Innovation and research.* Innovation and research is needed in order to improve the protection of critical infrastructure in Europe. This can include the development of improved risk assessment methodologies or even the development of new protection technologies. The EU is already promoting research and innovation in this area by way of such instruments as

the Pilot Project – Terrorism (1st call for proposals concerning CIP was published in January 2006) and the Preparatory Action for Security Research. These as well as other initiatives relevant for CIP will continue. Impacts would therefore be limited in this regard. Due to the existence of a common harmonized framework and the possibility to agree on research priorities, Option 4 would be likely (high) to stimulate research activities. The magnitude of the impact would be high as stakeholders would be very likely to invest in CIP research considering that a harmonized approach exists and there are agreed levels of protection among the Member States. Option 4 would be more likely (high) to promote greater resource efficiency than Options 1 and 2, as the existence of a harmonized CIP framework would help Member States agree on priorities. The magnitude of the impact would be high as research could concentrate on the single harmonized approach.

- Magnitude of the impact on the stimulation of research activities: - - -
  - Likelihood: √√√
- Magnitude of the impact on promoting greater resource efficiency in relation to research: - - -
  - Likelihood: √√√

Environmental impacts

Positive impact in terms of reducing environmental risks.The implementation of a harmonized CIP framework in each Member State would reduce the likelihood or scale of environmental risks (including the risk of fire, explosions, breakdowns, accidents and accidental emissions). The existence of a harmonized approach to the protection of key infrastructure in Europe under Option 4 would mean that the likelihood of this Option having an impact on the prevention of certain risks and consequences would be high. The magnitude of the impact (if it occurred) would be high.

- Magnitude of the impact on reducing the likelihood or scale of environmental risks: +++
  - Likelihood: √√√

Social impacts

- *Increasing security in the EU.* The implementation of CIP policies in the Member States would help decrease security risks concerning CI. As there would be a harmonized CIP framework in the EU, the Member States would have identical or similar levels of security concerning their critical infrastructure which would be high enough to limit associated risks. Nevertheless, the existence of a fully harmonized binding framework could also increase vulnerability as it could impede the building of trust among stakeholders, which is needed in order to comfortably exchange information on vulnerabilities. It is also true that having binding common levels of protection throughout the EU would mean that there might well be unnecessary protection measures put in place – or that there may be insufficient measures, as the threat levels are unlikely to be identical. The protection of critical infrastructure could then suffer. The likelihood of Option 4 having an impact on EU security is high. The magnitude of the impact on increasing security would be medium.
  - Magnitude of the impact on increasing EU security: ++

        - Likelihood: √√√

- *Stakeholder involvement*. The involvement of stakeholders in the development and implementation of CIP policies would be similar across the Member States as the harmonized framework would envisage stakeholder participation in the development and implementation of CIP measures. Nevertheless, the nature of the harmonization effort and the obligations imposed could discourage stakeholders from participating in the public-private dialogue as the potential outcome of such discussions would not have a sufficient effect on policy (most issues would have already been decided by way of the harmonization effort). The likelihood of Option 4 having an impact on stakeholder participation is medium. The magnitude of the positive impact of option 4 in this regard would be low (option 4 would be counterproductive).
    - Magnitude of the impact on stakeholder involvement: +
        - Likelihood: √√

- *Administrative setup*. The implementation of a CIP policy requires the adaptation of public authorities to dealing with CI related tasks. The implementation of Option 4 would mean that Member States would have to address CIP issues under the harmonized framework. All Member States would need to implement a certain number of modifications to their administrative structures. The likelihood of Option 4 having an impact on public administration is high. The magnitude would be high.
    - Magnitude of the negative impact on public authorities due to the necessity to adapt the administrative setup : - - -
        - Likelihood: √√√

- *Positive impact on employment and labour markets*. Employment and labour markets could be affected by the adoption of Option 4 similarly as under Option 3. A growing demand for security technologies and CIP research, as well as the implementation of certain CIP requirements may create new jobs. On the other hand most companies likely to be designated as critical infrastructure already fulfil similar obligations and have the necessary personnel to do it (business continuity plans are prepared; security officers exist). The magnitude of the impact would therefore be similar to that of Option 3. The likelihood of having a positive impact on employment markets would however increase to medium (as compared to Option 3).
    - Magnitude of the impact on employment and labour markets: +
        - Likelihood: √√

- *Building trust among stakeholders*. Building trust among all stakeholders involved in the CIP process is crucial for its long term success. Trust must be built among all stakeholders at both national and EU level. This process, although highly desirable, cannot be forced. The adoption of Option 4 could have the potential to discourage various stakeholders from participating and contributing to the development of CIP (strong regulatory measures do not build confidence among stakeholders). The likelihood of this impact occurring would be high. The magnitude would be low (Option 4 would not help build trust).
    - Magnitude of the impact on building trust among stakeholders: +

        - Likelihood: √√√

- *Improved protection of national critical infrastructure.* The adoption of Option 4 would require each Member State to take a series of specific measures in relation to their critical infrastructure. This would improve the protection of national critical infrastructure in general. Nevertheless, the adoption of a harmonized approach could destroy what has already been built in some Member States in terms of CIP. As a result, general protection could suffer. Consequently, the magnitude of the impact in terms of improving the protection of national critical infrastructure would be medium under Option 4. The likelihood of the identified impact would be high. .
    - Magnitude of the impact on improving the protection of national CI: ++
        - Likelihood: √√√
- *Improved protection of European critical infrastructure.* Option 4 would provide a framework for the identification and protection of European critical infrastructure and would impose specific measures on how to protect them. The framework would foresee the identification of European CI and relevant protection measures on a sector by sector basis. Option 4 would be very likely to introduce strong protection measures for European critical infrastructure.
    - Magnitude of the impact on improving the protection of European CI: +++
        - Likelihood: √√√
- *Improving the exchange of best practices.* The adoption of Option 4 could facilitate the exchange of best practices as a harmonized cooperation framework would exist. Full harmonization established through Option 4 could however raise the question whether there would be any need to exchange best practices, in a situation when a single harmonized approach would be used. As a consequence, the magnitude of the impact could be described as medium. The likelihood of its occurrence would be high.
    - Magnitude of the impact on improving the exchange of best practices: ++
        - Likelihood: √√√
- *Identification of interdependencies.* The identification of interdependencies is crucial in order to assess how various critical infrastructures interact and to identify potential vulnerabilities. Option 4, would facilitate the identification of interdependencies by way of setting priorities, providing funding, facilitating the exchange of information (like Option 3). Nevertheless, the likelihood would increase to high (as compared to medium under Option 3) as a coordinated effort would be made in this regard under the harmonized approach.
    - Magnitude of the impact on the identification of interdependencies: +++
        - Likelihood: √√√

Section 6: Comparing the options as to the general approach

Table of symbols

Table of symbols (distinguishes "-" for costs and "+" for benefits	
Small magnitude	- / +
Medium magnitude	-- / ++
Significant magnitude	- - - / +++
Low likelihood	√
Medium likelihood	√√
High likelihood	√√√
No impact	0

Summary table 1 – costs

Costs	Option 1 – no policy change	Option 2 – non binding framework	Option 3 – light legislative framework	Option 4 – full harmonization
Economic impacts				
Costs for businesses operating in a single Member State	- √√√	- √√√	- √√√	- √√√
Costs for businesses operating in more than one Member State	- - - √√√	Short/medium term: - - - Long term: - - Short/medium term: √√√ Long term: √√	- √√√	- √√√
Costs for authorities	- - √√√	- - √	- - √√	- - - √√√
Competition issues	- - - √√√	- - - √√	- √	- √
Social impacts				
Adaptation of the administrative setup	- - √√	- - √√	- - √√	- - - √√√

Summary table 2 – benefits

Benefits	Option 1	Option 2	Option 3	Option 4
Economic impacts				
Stimulation of research activities	+ √	+ √√	++ √√√	+++ √√√

Promotion of greater resource efficiency	+ √	+ √√	++ √√√	+++ √√√
Environmental impacts				
Reducing the likelihood or scale of environmental risks (fire, explosions etc)	++ √	++ √√	+++ √√√	+++ √√√
Social impacts				
Increasing EU security	+ √√√	+ √√√	+++ √√√	++ √√√
Stakeholder involvement	+ √	++ √	+++ √√√	+ √√
Employment and labour markets	0 0	0 0	+ √	+ √√
Building trust among stakeholders	+ √	+++ √√	+++ √√	+ √√√
Improved protection of national critical infrastructure	+ √√	++ √√	+++ √√	++ √√√
Improved protection of European critical infrastructure	+ √	++ √√	+++ √√	+++ √√√
Exchange of best practices	+ √	+++ √	+++ √√√	++ √√√
Identification of interdependencies	+ √	++ √√	+++ √√	+++ √√√

Advantages and drawbacks of the policy options

Policy options	Advantages	Drawbacks
Option 1: no policy change	▪ No need for new regulation. Regulatory environment does not change ▪ Member States remain completely free to address CIP issues as they see fit	▪ High costs for businesses operating in more than one Member State ▪ Competition may suffer as MS introduce various security obligations (companies in certain MS will have to spend less on CIP, while others more) ▪ Risk of costs for businesses associated with the implementation of CIP measures ▪ Small impact on improving EU security as accepted minimum

		levels of protection not achieved ▪ National and European CI not protected to a satisfying degree
Option 2: non-binding framework	▪ Trust can be built more easily among the stakeholders concerned ▪ No need for new regulation. Regulatory environment does not change ▪ Member States remain completely free to address CIP issues as they see fit	▪ High costs for businesses operating in more than one Member State ▪ Risk of costs for businesses associated with the implementation of CIP measures ▪ Competition may suffer as MS introduce various security obligations (companies in certain MS will have to spend less on CIP, while others more) ▪ Small impact on improving EU security as accepted minimum levels of protection not achieved
Option 3: light legislative framework	▪ Lower costs for businesses operating in more than one Member State ▪ Competition protected thanks to the existence of a minimum level playing field ▪ EU security strengthened ▪ Trust can be built more easily among the stakeholders concerned ▪ Improved protection of National and European CI	▪ Costs of establishment of new administrative structures ▪ Risk of costs for businesses associated with the implementation of CIP measures ▪ New regulatory environment is introduced.
Option 4: full harmonization	▪ Better stimulation of research activities and resource efficiency ▪ Improved protection of EU critical infrastructure ▪ Strong framework for the identification of interdependencies	▪ High costs of establishment of new administrative structures ▪ High costs of administrative reforms ▪ Difficult to build trust among stakeholders ▪ Risk of costs for businesses associated with the implementation of CIP measures

Would EU action have an added value?

As mentioned above, the European Council has already requested to Commission to prepare a European Programme for Critical Infrastructure Protection. The Member States therefore already see added value from EU level action in this regard.

Nevertheless, the analysis of the four policy options mentioned above confirms that action at European level would have an added value and is indeed needed. Each of the three policy options

which could be established at EU level (Options 2 to 4) could bring distinct benefits, but also a number of drawbacks.

Strengths and weaknesses of each policy option and preferred option

- Option 1. 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.
- Option 2. 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.
- Option 3. 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.
- Option 4. 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.

Based on the analysis above, policy option 3, the creation of a light legislative framework, would be the best policy option.

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.

Based on this assessment of broad policy options, the following section presents an assessment of possible contents of this framework.

Section 7: Analysis of impacts of specific measures under the recommended policy consisting of binding and non-binding measures

Overview

As set out above, the need for a comprehensive and consistent step-by-step approach to establishing EPCIP would merit a combination of binding and non-binding measures.

The following key issues could usefully be included in EPCIP:

- participation in CIP expert groups at EU level;
- use of a CIP information sharing process;
- identification and analysis of interdependencies;
- elaboration of national CIP programmes including the identification of national critical infrastructure;
- nomination of CIP Contact Points;
- identification and designation of European Critical Infrastructure;
- conducting threat and risk assessments for ECI
- elaboration of Operator Security Plans;
- designation of Security Liaison Officers.

Before analysing the specific impacts of the above mentioned key measures and assessing whether they should be implemented through non-binding or binding measures, it is useful to distinguish clearly between measures addressed to: a) the Member States, and/or b) to the owners/operators of ECI:

a) Member States: participation in CIP expert groups at EU level; use of a CIP information sharing process; identification and analysis of interdependencies; elaboration of national CIP programmes including the identification of national critical infrastructure; nomination of CIP Contact Points; identification and designation of European Critical Infrastructure; conducting threat and risk assessments for ECI.

b) ECI owners/operators: participation in CIP expert groups at EU level; use of a CIP information sharing process; identification and analysis of interdependencies; elaboration of Operator Security Plans; designation of Security Liaison Officers.

In the following section, for each of the key elements, the impacts of binding and non-binding instruments will be assessed. 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 will be weighed against the potential costs. In addition, in order to underline the importance of economic considerations, the potential impact on the functioning of the common market will also be assessed below.

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. As it is not possible at this time to assess what will be the level of participation of

stakeholders in these measures, it is also difficult to foresee potential costs. Nevertheless a number of general comments can be made concerning the key non-binding measures.

Analysis of impacts of key measures forming part of the EPCIP framework

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. The use of EU level expert groups in order to bring together relevant stakeholders would greatly facilitate a CIP information exchange. Such CIP expert groups would have a very positive impact in terms of security as they could:

    - 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;
    - Facilitate 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.

    Costs would be limited as CIP expert groups would only be setup where needed and on a *pro bona* basis, and would not replace other existing groups already established or which could be adapted to fulfil the needs of EPCIP. Moreover, CIP expert groups would be formed in order to achieve a clearly identified objective and would be dissolved following its attainment.

    The creation of EU level expert groups would not have an impact on the Common Market.

    As EU level expert groups would function on a voluntary basis, they should form part of the non-binding framework of EPCIP. Binding measures would be contrary to the nature of such voluntary groups.

2. *Use of a secure 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 have been shared voluntarily will not be publicly disclosed and that that sensitive data is adequately protected. 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. Consequently, a non-binding approach would be preferred.

    Making sure that the CIP information exchange is secure will of course have a positive impact on increasing security. Costs can be expected to remain low as the measures remain non-binding and are relevant more for an introduction of a certain security oriented "state of mind". Consequently, the process should amount to the development of guidelines on information handling etc.

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. A binding approach could therefore be counterproductive.

This ongoing process will feed into the assessment of vulnerabilities, threats and risks concerning critical infrastructure in the EU and may therefore have a significant impact on security. An estimation of costs cannot be made at this time as the process of identifying interdependencies is of an ongoing nature. It is worth underlining nevertheless that EU funding could contribute to this process by way of calls for proposals.

4. *Elaboration of National CIP Programmes*. Raising CIP capability and improving the protection of critical infrastructure in the EU are objectives of EPCIP. 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. The Commission should support the Member States in their NCI related efforts where requested and where possible.

   The impact of NCI related measures on security and costs will of course be different depending on whether a binding or non-binding approach to NCI is introduced in EPCIP.

   - Impact of a binding approach concerning the elaboration of National CIP Programmes. Under this scenario, EPCIP would oblige each Member State to create a National CIP Programme based on a number of minimum general requirements and on the list of CI sectors relevant for EPCIP. This obligation would be put forward in EPCIP in order to ensure that each Member State develops a coherent national approach to CIP and that this national approach is compatible with EPCIP (and thereby with the approaches of the other Member States). The relevant binding provisions would nevertheless be general enough to allow each Member State to make use of national specificities.
     - Security. In terms of the impact on security, the elaboration of National CIP Programmes under a binding framework could be expected to have a strong effect on increasing the security of critical infrastructure in Europe because:
       - All Member States would be required to establish National CIP Programmes addressing similar issues. This would mean that those Member States which already have such programmes would have to assess whether they fulfil the common minimum requirements under EPCIP. Those Member States which do not have such programmes would have to develop them.
       - Since all National CIP Programmes would address similar issues, the programmes would be compatible and comparable with each other.
       - Similarity between the National CIP Programmes in terms of the approach used would guarantee that each Member State is sufficiently addressing national CIP issues.
     - Costs. The costs associated with National CIP Programmes should be separated into two distinct phases: the elaboration phase and the implementation phase. The costs of both phases would vary in each Member State.
       - The elaboration phase would be limited to the drafting of the National CIP Programmes. This phase would therefore only require funding concerning the

elaboration of a national approach to CIP. It should be expected that this work can be fulfilled by the regular administrative structures usually dealing with CIP in a particular Member State. Those Member States which already have relevant programmes would simply need to make sure that they take into account the minimum common requirements. Those Member States which would have to elaborate a completely new programme would have to incur higher costs, although these would generally be of an administrative nature. Although quantification of this process is not possible at this time, the costs should be expected to remain low during this phase.

- The implementation phase would require a higher degree of funding. The costs would vary among the Member States depending on the level of advancement on CIP issues (e.g. several Member States have already identified their National Critical Infrastructure and are already engaged in dialogue with CI owners/operators). Importantly nevertheless, some of the minimum requirements of the National CIP Programmes specified in the EPCIP proposal could be funded by the Commission (e.g. studies on interdependencies).

- There would be no direct impact on the functioning of the common market as a result of this obligation. Indirectly however, the fact that comparable programmes would be setup concerning NCI would lead to similarities in protection measures concerning NCIs. This in turn would help approximate national security requirements for NCIs (level playing field).

- Impact of a non-binding approach concerning the elaboration of National CIP Programmes. Under this scenario each Member State would be encouraged to create a National CIP Programme. A non-binding instrument would propose a number of issues which could be taken into account by the Member States when developing such programmes including the identification of NCI.

  - Security. In terms of the impact on security, the elaboration of National CIP Programmes could be expected to have a positive impact on increasing the security of critical infrastructure in Europe as each Programme would set out a Member State's strategy toward CI protection and would confirm that the issue is being addressed to a certain extent. At the very minimum, such Programmes would serve as a good awareness raising tool. The positive impact on security could however be expected to be lower than under a binding approach as the Member States would most likely develop a number of approaches to the protection of National Critical Infrastructure which may be incompatible between each other. This would hinder certain forms of cooperation (e.g. exchange and comparability of certain types of information). Moreover, certain Member States could refrain from developing such programmes.

  - Costs. The costs associated with National CIP Programmes cannot be assessed as the approaches of the Member States will vary. Nevertheless, the elaboration costs can be expected to remain low. Implementation costs will depend on the ultimate contents.

  - There would be no impact on the functioning of the common market.

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.

In conclusion, the use at first 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. As mentioned above in the analysis of the need to create National CIP Programmes, either a binding or non-binding approach to NCI could be used in this regard.

   - Impact of a binding approach concerning the identification of NCI. Under this scenario, EPCIP would oblige the Member States to ensure the ongoing identification of National Critical Infrastructure. Such an obligation would be introduced in order to make sure that all Member States are aware of the critical infrastructure assets located within their territory and understand the potential consequences of the loss or disruption of such an infrastructure. In general terms, the Commission would not require specific information concerning these critical assets (with due regard to existing Community competences).
     - Security. The identification of national critical infrastructure by each Member State would have a very strong effect on improving the security of critical infrastructure in Europe. This would be the result of the fact that each Member State would have to go through a process of assessing which concrete infrastructure are critical for it and why. This would of course result in increasing the level of understanding of CIP issues within the Member States.
     - Costs. The costs of identification would vary among the Member States. Those Member States which have already identified their National Critical Infrastructure would not have to repeat the process. Those Member State which have not completed the necessary identification, would incur costs associated with the collection and analysis of the relevant data. The associated costs for infrastructure owners/operators would be very low as it can be reasonably expected that they already know what assets are critical for them. The costs would remain low.
     - This provision would not have an impact on the functioning of the common market.
   - Impact of a non-binding approach concerning the identification of NCI. Under this scenario, EPCIP would encourage the Member States to identify their National Critical Infrastructure, but the Member States would be under no obligation to do so.
     - Security. The non-binding approach would clearly have a lower security impact than a binding approach as there would be a risk that not all Member States would address the NCI issue sufficiently. Nevertheless, the need for a step-by-step approach to EPCIP and the need to concentrate on ECI may merit the use of a non-binding approach. The issue of encouraging the Member States to identify their NCI could then be integrated within the non-binding provisions concerning National CIP Programmes. Costs would vary depending on the types of actions undertaken by each particular Member State.
     - Costs. The costs of identification would vary among the Member States as under the binding measures.
     - This provision would not have an impact on the functioning of the common market.

In conclusion, 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.

   - Impact of a binding approach concerning the nomination CIP contact points:

     - Security. From the security perspective, this provision is important as it envisages the designation of a horizontal CIP coordinator in each Member States, which would have a general overview of CIP related activities in that Member State and would function as the single point of contact on CIP issues. A horizontal overview of CIP activities is needed in order to encourage compatible and adequate approaches to CIP in all CIP sectors. In addition, the CIP Contact Points would represent the Member States in the Committee setup under a binding EPCIP instrument, which would take decisions on implementation measures under the binding instrument. The CIP Contact Points would also represent the Member States in the informal CIP Contact Group being setup under the horizontal EPCIP framework and would therefore contribute to the development of EPCIP. The nomination of a single contact point would be important in terms of building trust and facilitating discussions on CIP issues at the EU level.
     - Costs. The cost of nominating a single CIP contact point will vary in each Member State as a consequence of different administrative structures and salary levels. In general terms, two situations should be differentiated:
       - A civil servant already employed by the public administration and already dealing with CIP issues is nominated as the CIP Contact Point. The costs here would be negligible as the necessary structures would already be in place. The coordinating role of the Contact Point would require the establishment of contacts with all the relevant CIP authorities in a particular Member States. This would be the case for most of the Member States.
       - A new position is created within the public administration. Costs would vary between the Member States, but would generally result from the need to incur administrative costs.

       Costs can reasonably be expected to remain low as 23 Member States have already nominated their CIP contact points and have notified the names to the Commission.
     - This provision would not have an impact on the functioning of the common market.

   - Impact of a non-binding approach concerning the nomination CIP contact points on:

     Security. From the security perspective, the nomination of CIP Contact Points is crucial for the success of EPCIP. Without participation of all Member States in the process, the objective of improving the protection of CI in Europe will not be achieved. The main problem with a non-binding approach would be that the Member

States would be free to decide on whether to actually nominate such a Contact Point. The lack of even a single Member State in the EPCIP process would risk derailing the project. From this perspective the benefit for security of a non-binding approach would be low.

- Costs. The cost of nominating a single CIP contact point will vary in each Member State. The costs would be similar as under the binding approach given that a Member State would nominate a Contact Point.
- This provision would not have an impact on the functioning of the common market.

Consequently, 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. The identification and designation of European Critical Infrastructure could best be done based on a four step process:

    i. The development of criteria to identify ECI on a sectoral basis;

    ii. The adoption of the criteria

    iii. The identification by the Member States of those critical infrastructure which could satisfy the common criteria;

    iv. The formal designation of specific infrastructure as ECI.

This process would lead to the creation of a list of European critical infrastructure which if disrupted or destroyed would have serious consequences for the entire Community, two or more Member States, or a single Member State if the critical infrastructure is located in another Member State.

- Impact of a binding approach concerning the identification and designation of ECI:
    - Security. The security benefit of the identification and designation of ECI can be expected to be very big as this identification is a prerequisite for improving the protection of such infrastructure (if needed). This has to be done using a commonly agreed approach with the full participation of all Member States.
    - Costs. The costs involved would be small as they would generally be of an administrative nature associated with the holding of meetings and facilitating discussions especially in the criteria development phase.
    - This provision would not have an impact on the functioning of the common market.
- Impact of a non-binding approach concerning the identification and designation of ECI on:
    - Security. The potential security benefit would only be achieved if the process of identification actually took place. As it is unlikely that such a process could be

completed to a satisfactory degree under a non-binding approach the security benefit would be low.

- Costs. The potential costs would be the same as those under a binding approach.
- This provision would not have an impact on the functioning of the common market.

In conclusion, 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 as:

- Relevant information concerning identified threats and risks could be communicated to the ECI via the Security Liaison Officer, thereby strengthening an ECI's CIP capacity.
- The information would help the MS prepare the generic sectoral summaries of identified vulnerabilities, threats and risks which would be submitted to the Commission.

➢ Impact of a binding approach to conducting vulnerability, threat and risk assessments for ECI:

- Security. The security benefit would be large as the Member State, the ECI owner/operator and the Commission could benefit from the vulnerability, threat and risk assessments and act upon it. The binding framework would foresee the use of this information in order to achieve greater CI security. All Member States would fully participate in the process so weak links would be eliminated to the highest possible extent.
- Costs. The costs of conducting such assessments would vary among the Member States and among the various CIP sectors. Nevertheless, it can be expected that such assessments would be made as part of regular work conducted by law enforcement agencies of the Member States. The additional costs would therefore be low.
- This provision would not have an impact on the functioning of the common market.

➢ Impact of a non-binding approach to conducting vulnerability, threat and risk assessments for ECI:

- Security. The security benefit would not be as significant as under the binding approach as there would be no binding provisions concerning the sharing and use of this information. It would therefore not be possible to conduct an EU level analysis of security gaps and it would not be possible to propose measures to address these gaps.
- Costs. The costs of conducting such assessments would vary among the Member States and among the various CIP sectors. Costs would remain low as under the binding approach.
- This provision would not have an impact on the functioning of the common market.

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. The essence of the European Programme for Critical Infrastructure Protection would be lost without the implementation of this measure.

9. *Obligations of European Critical Infrastructure.* In order to achieve the objective of improving the protection of ECI, two 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.

➢ Impact of binding obligations for ECI on:

- Security. Security would clearly benefit from these provisions as:
  - European critical infrastructure would have to complete the process of preparing Operator Security Plans which make sure that risk, threat and vulnerability assessments are sufficiently taken into account and that the owner/operator is aware of its critical assets and knows how best to protect them. The information from the OSPs would help the Member States elaborate generic reports concerning vulnerabilities, threats and risks to ECI, which would be submitted to the Commission with a view to identifying gaps in protection measures.
  - The designation of Security Liaison Officers would facilitate the CIP process as each owner/operator of European critical infrastructure would have a clearly identifiable official responsible for CIP issues. This official would not only be the single point of contact with the authorities concerning CIP, but would also contribute to the development of CIP policies by way of participating in expert/stakeholder meetings (building trust).
- Costs. The costs would vary among the Member States. Although exact quantification is not possible, the following assumptions can be made concerning the two above mentioned obligations:
  - The owners/operators of European critical infrastructure would incur costs associated with the preparation of Operator Security Plans. The exact costs will vary considerably depending on the sector concerned, the type of activities being undertaken, the level of preparedness already achieved. Costs can be expected to be low or non-existent for those owners/operators who:

- Have already prepared business continuity plans.
- Are located in a Member State with an already advanced CIP programme (e.g. in certain Member States an obligation for national critical infrastructure to prepare Operator Security Plans already exists).
- Belong to a sector already possessing certain security/safety obligations (e.g. the Port Security Directive[2] obliges port authorities to develop port security assessments and plans which would most likely already satisfy the obligations imposed through a sector specific Operator Security Plan).

Costs can reasonably be expected to be higher for owners/operators who have not addressed security or business continuity issues at all. It could however be expected, that even without the adoption of EPCIP, certain costs concerning business continuity plans would be incurred at a certain point in the future. The problem would remain however that this would be done in an uncoordinated and incomparable fashion.

Recognising the need for a cost-effective system EPCIP should be based on a sectoral approach and should build on existing sectoral measures. With this in mind, the specific contents of the Operator Security Plans would be elaborated on an individual basis taking into account (where relevant) existing CIP sector specificities (e.g. port security assessments and plans under the Port Security Directive). A procedure would be established foreseeing the exemption of certain sectors from the obligation to elaborate OSPs.

- The owners/operators of European critical infrastructure would incur costs associated with the designation of Security Liaison Officers. As with the Operator Security Plans however, these costs will vary depending on a number of factors. Costs can be expected to be low or not to exist at all for those owners/operators who:
  - Already possess a security officer. For most owners/operators likely to be designated as ECI, this is most likely the case. In this situation, the designation of an SLO will simply amount to giving particular security officials additional competences.
  - Are located in a Member State with an already advanced CIP programme (e.g. in certain Member States an obligation for national critical infrastructure to designate SLO already exists).
  - Belong to a sector already possessing certain security/safety obligations (e.g. the Port Security Directive[3] already obliges the Member States to appoint port security officers for each port. Although

[2] Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security.

[3] Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security.

this is not identical to the designation of a SLO, which has to be done by the owners/operator, it can serve as a basis for such a designation).

Costs will of course be higher for those owners/operators which do not possess any security officers. Such a situation would however be relatively unlikely for owners/operators designated as European critical infrastructure.

- These obligations could have an impact on the functioning of the common market. Introducing similar obligations for all ECI would mean the existence of a level playing field for all ECI owners/operators in the EU. In other words, the use of binding measures would make sure that all ECI owners/operators are subject to the same rules as opposed to having varying obligations in particular Member States.

➢ Impact of non-binding obligations for ECI on:

- Security. The security benefit would be low mainly as a consequence of the fact that only certain ECI owners/operators would comply with the obligations. This would hinder the process of improving the security of ECI as:
  - Without having each ECI develop OSPs, it will not be possible to conduct an analysis of gaps and it will not be possible to propose measures on how to address them. Moreover, without an OSP, it will be difficult to assess whether the ECI owner/operator is addressing security issues to a satisfactory degree, which raises the issue of having weak links in the security of the EU.
  - In relation to the designation of Security Liaison Officers, the fact that certain ECI owners/operators would not have SLOs would hinder the development of security measures as it would be difficult to ensure the needed communication concerning security issues. The lack of a specific person responsible for CI security would also hinder the process of building trust among stakeholders, which is needed in order to comfortable exchange information.
- Costs. The costs would depend on whether the measures were actually implemented. If so, they could be assessed as under the binding approach. If no, then under a non-binding framework ECI owners/operators would still be subjected to varying basic obligations depending on the Member State in which they operate. This would lead to ECI owners/operators having to invest in different measures depending on the Member State in which they operate. The negative impact on costs could therefore even be larger than under the binding option.
- The use of non-binding measures could have an impact on the functioning of the common market. As certain ECI owners/operators would implement the measures, others would refrain and would thereby gain a competitive advantage over others. The use of non-binding measures could also encourage the Member States to develop various incompatible obligations. Under such a scenario, ECIs could end up being subjected to a number of different security requirements in each of the Member States.

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.

Summary table

Table of symbols (distinguishes "-" for costs and "+" for benefits	
Positive impact	+
Negative impact	-
No impact	+/-
Not applicable	n.a.

Key provision	**Binding approach**			**Non-binding approach**			**Other considerations**
	Impact on:			Impact on:			
	Security	Costs	Common Market	Security	Costs	Common Market	
Participation in CIP expert groups at EU level	n.a.	n.a.	n.a.	+++	+/-	n.a.	
Use of a CIP information sharing process	n.a.	n.a.	n.a.	+++	+/-	n.a.	
Identification and analysis of interdependencies	n.a.	n.a.	n.a.	+++	n.a.	n.a.	
Elaboration of National CIP Programmes	+++	-	+	+	n.a.	n.a.	Need to concentrate first on ECI
Identification of National Critical Infrastructure	+++	+/-	n.a.	+	+/-	n.a.	Need to concentrate first on ECI
Nomination of CIP Contact Points	+++	+/-	n.a.	+	+/-	n.a.	
Identification and designation of European critical infrastructure	+++	+/-	n.a.	+	+/-	n.a.	
Conducting threat and risk assessments for ECI	+++	+/-	n.a.	+	+/-	n.a.	
Designation of a Security Liaison Officer, elaboration of an operator security plan	+++	-	+	+	--	-	

Conclusions

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 analysed above, 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).

As mentioned above, the horizontal non-binding EPCIP framework could be established by way of a Commission Communication. The Communication would clearly specify that EPCIP consists of:

1. A Directive concerning ECI
2. Non-binding measures designed to facilitate the implementation of EPCIP, including an EPCIP Action Plan, the use of CIP expert groups at EU level, CIP information sharing process and the identification and analysis of interdependencies.
3. A possible Critical Infrastructure Warning Information Network (CIWIN) (this will be the subject of a separate proposal)
4. Non-binding measures which may optionally be used by Member States for National Critical Infrastructure (NCI) under their responsibility
5. Accompanying financial measures set out in the EU programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" (financial perspectives for 2007-2013). This programme will provide funding opportunities for CIP related measures having a potential for EU transferability

A binding instrument concerning ECI would constitute a key element of the EPCIP package as set out in the EPCIP Communication. The instrument, which would take the form of a Directive, would only be limited to the identification and designation of European Critical Infrastructure, and to establishing a common approach to the assessment of the needs to improve the protection of such infrastructure.

In particular such a Directive would address the following issues:

1. The establishment of a procedure for the identification and designation of European critical infrastructure
2. The elaboration of an operator security plan and the designation of a Security Liaison Officer by each owner/operator formally designated as an ECI in order to conduct vulnerability, threat and risk assessments
3. The establishment of a reporting mechanism under which each Member State would provide the Commission with a generic overview of vulnerabilities, threats and risks encountered in each CIP sector.
4. The nomination by each Member State of CIP contact points.

In comparison with the light legislative framework foreseen under Option 3, this approach would introduce the following modifications:

1. The Directive would only be limited to establishing a procedure for the identification and designation of ECI and the assessment of their vulnerabilities
2. National Critical Infrastructure would be completely left out of the Directive. A general approach to NCI would be provided in the Communication on EPCIP, but the Member States would be free to decide whether such an approach would suite them.
3. The procedure for the development of specific protection measures would be completely left out of the framework. The development of such measures could be the objective of future policy and/or legislative exercises, if appropriate. The information gathered under the EPCIP framework could contribute to this process nevertheless (e.g. for the preparation of an impact assessment).

The number of CIP sectors included in the Directive would be reduced as certain NCI-relevant sectors would no longer be included.

Table 1: Binding and non-binding EPCIP measures and division of responsibilities among stakeholders

Key provision	**Stakeholder responsible**		
	Member State	European CI	EC
Non-binding measures			
Participation in CIP expert groups at EU level	√	√	√
Use of a CIP information sharing process	√	√	√
Identification and analysis of interdependencies	√	√	√
Elaboration of National CIP Programmes	√		
Identification of National Critical Infrastructure	√		
Binding measures			
Nomination of CIP Contact Points	√		
Identification and designation of	√		√

European critical infrastructure			
Conducting threat and risk assessments for ECI	√		
Designation of a Security Liaison Officer, elaboration of an operator security plan		√	

Proposed timeframe for implementation

1. The sectoral criteria for the identification of ECI would be adopted at the latest one year after the entry into force of the ECI Directive.
2. Each Member State would identify the relevant critical infrastructure which satisfy the agreed criteria and notify this list to the Commission at the latest one year after the adoption of the relevant criteria.
3. Within 6 months of the above mentioned identification, the Commission would propose a list of critical infrastructure to be designated as ECI.
4. Within 1 year after designation as ECI each ECI owner/operators would submit its Operator Security Plan to the relevant Member State authority.
5. Within 1 year after designation as ECI each ECI owner/operators would designate its Security Liaison Officer
6. Within 1 year after designation as ECI, each Member State would conduct a risk and threat assessment in relation to that ECI.
7. Within 18 months after designation as ECI, each Member State shall report to the Commission on a summary basis of the types of vulnerabilities, threats and risks encountered in each CIP sector.

Section 8: Monitoring and evaluation

Core indicators of progress

The following achievements could be used to assess progress being made on CIP issues at a horizontal level. Other progress indicators would have to be used in order to assess progress being made in the various sectors (under the sector-by-sector approach).

- Establishment of a CIP contact group composed of representatives of all Member States and relevant Commission services
- Elaboration of common CI sector-based working definitions and terminology
- Creation of an inventory of existing national, bilateral and EU critical infrastructure protection programmes
- Establishment of a list priority sectors/infrastructure that appear most critical at the European level, taking into account interdependencies
- Creation of guidelines on collection and use of sensitive CIP data between Commission, Member States, owners/operators and other relevant parties
- Setting up, where relevant, of CIP sector based expert groups/networks at EU level
- Identification of gaps where Community initiatives would have added-value
- Initiation of EU funding for CIP actions

Possible monitoring and evaluation arrangements

Evaluation and monitoring of the implementation of EPCIP would be a multi-level process requiring the involvement of all stakeholders:

- 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.
- The Commission could report progress to MS and other institutions each calendar year in a Commission staff working paper.
- Each Member State could prepare an annual report concerning the overall implementation of EPCIP under its jurisdiction and assessing compliance with its National CIP Programme. These reports would be submitted to the Council and the Commission.

Annex 1: Results of the EPCIP Green Paper – Member State comments

Twenty-two Member States provided official responses to the EPCIP Green Paper consultation process.

The Member States welcomed the Commission's initiative and work on the development of the European Programme for Critical Infrastructure Protection. The national responses to the EPCIP Green Paper supported the fundamental approach of addressing the issue of critical infrastructure protection (CIP) from a European perspective and of developing a European Programme for Critical Infrastructure Protection (EPCIP). The need for increasing the critical infrastructure protection capability in Europe and helping reduce vulnerabilities concerning critical infrastructure was acknowledged. The importance of the principle of subsidiarity was repeatedly stressed in the responses of the Member States.

The EPCIP Green Paper has proved to be a useful instrument in terms of aiding the launch of national discussions concerning critical infrastructure protection.

Goal of EPCIP

The Member States were divided concerning the appropriateness of the goal for EPCIP formulated in the Green Paper. Those Member State which were not satisfied with the presented goal generally emphasised that it is the responsibility of each Member State, and not of a European programme, to guarantee the security of critical infrastructure. Consequently the broad goal of EPCIP should be to raise CIP capability and improve the protection of critical infrastructure in Europe.

Scope of EPCIP

The Member States generally supported the adoption of an all-hazards approach for EPCIP with terrorism being a priority.

Key principles

The Member States generally supported the five key principles listed in the EPCIP Green Paper although a number of modifications and additions were proposed.

Common EPCIP framework

A majority of Member States found that a common EPCIP framework would be an effective tool in strengthening CIP capability in Europe. The Member States were of the opinion that the common framework would be useful in terms of clarifying the responsibilities of the stakeholders concerned. The key role and responsibility of the Member States in this process was repeatedly stressed. The Member States were evenly divided concerning the need for a legislative package for EPCIP. The idea of developing legislation in the future was not ruled out. The Member States were also divided as to the question whether the EPCIP framework should be voluntary or obligatory with a larger number of Member States opting for the obligatory approach.

The Member States generally agreed on the need to have a sector-by-sector approach to the specific provisions of EPCIP. The Member States were generally pleased with the list of critical infrastructure sectors and the list of definitions included in the Green Paper and saw them as a good basis for discussion.

Definition of EU critical infrastructure

The Member States were evenly divided on whether European Critical Infrastructure (ECI) should be defined as infrastructure having a potentially serious cross-border impact on two or more, or three or more Member States. Several Member States emphasised that the definition of ECI should not only be based on the number of Member States affected. The importance of bilateral agreements was also emphasised.

Interdependencies

The importance of identifying interdependencies at various levels was acknowledged by the Member States. Several Member States emphasised the difficulty of this task.

Implementing steps for ECI

The implementing steps concerning ECI were generally seen as useful by a majority of Member States although some responses indicated that it may be too early to clearly define this process. The role of the Commission was generally seen as that of an active participant and facilitator of the EPCIP process.

The NCI role in EPCIP

The Member States were divided concerning the inclusion of NCI in the EPCIP framework. Around half of the Member States saw added value in having EPCIP address NCI at least by way of promoting the exchange of best practices and the building of generic knowledge. Several Member States underlined that EPCIP would have to deal to a certain degree with NCI as it would be infrastructure already designated by a Member State as National Critical Infrastructure which would additionally be designated as European Critical Infrastructure. Around half of the Member States were of the opinion that the best relationship between EPCIP and NCI would be to allow the use of parts of EPCIP as needed in relation to NCI, but that there would be no obligation to do so.

National CIP programmes

The Member States emphasised the need for the development of National CIP Programmes. More than half of the Member States thought that EPCIP could play a positive role in the development of National CIP Programmes either by being the basis for such programmes or inspiring them.

Single overseeing body

All Member States agreed that it is the responsibility of each Member States to designate and manage CI under its jurisdiction. The Member States clearly saw added value in the creation of either a single overseeing body or a single contact point for CIP. Over half of the Member States supported the idea of having a single overseeing/coordination body in each Member State. Several underlined that such bodies already exist.

Implementing steps for NCI

The Member States were generally supportive of the list of implementing steps concerning National Critical Infrastructure proposed in the Green Paper although a number of modifications were proposed.

Responsibilities of CI owners/operators

In general, a majority of Member States found the list of potential responsibilities for CI owners/operators as acceptable. A number of Member States mentioned however the need to

separate the rights/obligations of ECI and NCI. A majority of Member States found the concept of developing Operator Security Plans (OSP) as useful, at the very least, as an example of a best practice. The Member States proposed a number of potential rights which could be given to CI owners/operators.

Dialogue with CI owners/operators

The Member States generally agreed on the need to engage in a public-private dialogue concerning CIP. This dialogue should be conducted at MS level and at EU level on a sector-by-sector basis. At EU level, the private sector should be represented by the relevant industry associations. A number of Member States emphasised the importance of having a voluntary approach to the issue of public-private dialogue. Only through a voluntary partnership, will sufficient levels of trust be built.

Common methodologies

Around half of the Member States saw added value in the idea of harmonizing or calibrating alert levels in the EU and in developing common methodologies of identifying and classifying threats, capabilities, risks, and vulnerabilities and drawing conclusions about the possibility, probability, and degree of severity posed by a threat.

Funding

The Member States did not offer any estimates concerning the costs of implementing the proposals put forward in the EPCIP Green Paper.

Evaluation and monitoring

The Member States generally indicated their support for some form of evaluation mechanism.

Annex 2: Results of the EPCIP Green Paper – comments from industry associations

Nineteen European-level and international industry associations provided comments to the Green Paper on the European Programme for Critical Infrastructure Protection (EPCIP). In addition to a general European business response, a number of industry sectors provided comments:

- Energy sector – responses from five associations
- Transport – responses from seven associations
- IT – responses from two associations
- Water – response from one association
- Chemical - response from one association
- Tank Storage - response from one association
- Security - response from one association

The industry associations generally provided comments on some of the ideas contained in the EPCIP Green Paper, but usually did not respond to the questions posed in the document. Nevertheless a number of messages seemed to be of key concern for them:

- The industry generally supports the creation on an EU-wide EPCIP framework designed to increase the security of critical infrastructure in Europe
- EPCIP must minimize any negative impacts on business competitiveness;
- Duplication of efforts must be avoided;
- The industry underlined the absolute need to be involved from the very outset on the development of EPCIP considering that a majority of critical infrastructure are owned by the private sector;
- A sector-by-sector approach must be pursued in the development of the specific parts of EPCIP;
- Confidentiality is extremely important

The industry associations are generally keen to participate in the dialogue and development of EPCIP.

The transport sector had generally a positive view concerning the EPCIP initiative and the need to address the issue from a European perspective. Nevertheless two of the seven responses, representing a part of the aviation sector and a part of the freight sector, seem to have been provided for the sole purpose of arguing that they should not be covered by anything in EPCIP because they are already contributing to security.

The energy sector underlined the need to conduct a detailed assessment of the situation existing in the energy sector in order to identify gaps and possible solutions. The sector underlined the absolute need for a sectoral approach in addressing CIP issues as several specificities of the sector were mentioned in the responses. The energy sector also emphasised the importance of confidentiality, as public discussions on CIP related issues may increase the vulnerability of certain infrastructure.

The IT and water sectors were generally supportive of the need to improve the security and protection of CIs and expressed their interest in participating in the development of EPCIP.

The chemical sector was also generally supportive but underlined the need to avoid duplication of efforts citing the existence of several instruments which already increase the security and safety of the sector.

The tank storage industry generally felt that its sector should fall outside the remit of EPCIP.

The security industry was generally supportive of the ideas contained in the EPCIP Green Paper and underlined the need for an EU framework addressing CIP issues, based on the experience and expertise of national CIP-efforts.

Goal of EPCIP (question 3.1)

The transport sector provided few concrete comments on this issue. It seems however that the transport industry felt that the goal of EPCIP should be revised. According to one response, the provision of "adequate and equal levels of protective security" is an unrealistic goal considering the differences existing between sectors and the need for effectiveness. One transport association moreover mentioned that EPCIP should facilitate the work of the Member States in the CIP field.

The energy sector did not provide detailed comments on this issue. One response pointed out however that the attainment of "equal levels of protective security" is unrealistic.

The IT sector, water sector and the security industry found the objective identified in the Green Paper as adequate.

The tank storage industry and the chemical industry did not provide comments on this issue.

Scope of EPCIP (question 3.2)

The EPCIP Green Paper posed the question whether EPCIP should be based on an all hazards approach, an all-hazards approach with a terrorism priority or a terrorism hazards approach. The general business view was that EPCIP should have an all-hazards focus, but that it must be sufficiently flexible to deal with the specificities of terrorism.

The transport sector was divided on this issue:

- One response supported the option of basing EPCIP on an all-hazards approach with a terrorism priority;
- One response supported the all-hazards approach
- One response supported the terrorism-hazards approach.

Most of the energy industry would like to restrict the scope of EPCIP to terrorism. This view was expressed in four responses. Two response from the energy sector also emphasised the need to eliminate consequence management from the scope of EPCIP.

The IT sector supported having an all-hazards approach with a terrorism priority. One industry association underlined nevertheless, that if this option is chosen, it must be made clear that other non-terrorist hazards are not put aside.

The security industry would support having an all-hazards approach.

The tank storage industry, water sector and the chemical industry did not provide comments on this issue.

Key principles (question 4)

The EPCIP Green Paper listed five key principles: subsidiarity, complementarity, confidentiality, stakeholder cooperation and proportionality.

The general business position was that it agreed with list of key principles. The principle of confidentiality was stressed as being of crucial importance.

The transport sector generally supported the list of key principles, but suggested a number of slight clarifications.

There was general agreement among the energy related associations on the key principles, but there was particular concern about confidentiality and that any measures should be proportional to risk.

The IT, water, security and tank storage sectors generally supported the list of key principles.

The chemical industry association did not offer comments on this issue.

Common EPCIP framework (question 5)

The EPCIP Green Paper raised several issues concerning the need and format of a potential EPCIP framework in the EU.

The general business position was that an EU EPCIP framework should be established.

The transport sector generally supported an EU approach to identifying ECI through a common framework, including common definitions and principles. However there was no agreement on whether this should be voluntary or mandatory.

The energy sector generally agreed that some form of common framework would be necessary, with those favouring a legislative framework feeling this is needed for setting definitions and responsibilities. No organisation disagreed with the sectoral approach proposed in the Green Paper.

The IT sector supported the idea of having a common EPCIP framework, but was divided on the specific approach to be taken. One response mentioned that if a legislative approach was to be adopted, it should only contain the basic aspects of EPCIP. Another response underlined that the EU framework should be limited to the exchange of best practices.

The tank storage industry supported the idea of a common framework. On the issue of legislation, this industry felt that a step-by-step approach would be preferred with ideas with being tested and then being implemented through legislation.

The security industry supported the idea of having a common framework on CIP. The industry felt that a voluntary approach would be ideal.

The water and chemical industry associations did not offer specific comments on this issue.

The industry generally felt that a framework would be helpful but seemed afraid of overregulation and duplication.

Definition of EU critical infrastructure (question 6.1)

The general business position was that European Critical Infrastructure (ECI) should relate to two or more Member States.

The EU transport industry associations did not provide detailed comments on this. Two responses nevertheless favoured the 2 or more approach.

The energy sector favoured that EPCIP should deal with 3 or more Member States underlining that bilateral agreements should be sufficient to address of CIs.

The IT sector and the security sector supported the 2+ approach.

The water, tank storage and chemical industries did not provide an answer to this issue.

Interdependencies (question 6.2)

The general business position was that interdependencies should be identified at both the national and EU level.

The transport sector did not provide clear comments concerning interdependencies apart from stating that there is no universal approach to the issue and that they are not aware of any concrete methodologies.

The energy sector generally expressed the view that the process of identification of interdependencies should involve all stakeholders and should initially take place at national level.

The IT industry only underlined the need to involve all stakeholders in the process.

The security industry was of the opinion that interdependencies should first be tackled at the national level.

The water, tank storage and chemical industries did not provide an answer to this issue.

Implementing steps for ECI (question 6.3)

The general business position was that the list of implementing steps is fairly complete, but it should also ensure a regular revision of criticality.

The transport sector did not offer concrete comments on whether the list of implementing steps for ECI would be acceptable. Two responses underlined however the need for an arbitration mechanism in case one MS would like to designate a particular infrastructure located in another MS as ECI.

The energy sector was generally supportive of the general implementing steps for ECI contained in the Green Paper.

One response from the IT sector felt that the list of steps was too simple.

The security industry generally supported the list of steps but underlined that private partners should be involved more in the process.

The water, tank storage and chemical industries did not provide an answer to this issue.

The NCI role in EPCIP (question 7.1)

The EPCIP Green Paper raised the issue of what should be the relationship between EPCIP and National Critical Infrastructure.

The general business position was that national critical infrastructure (NCI) should be interrelated with EPCIP in order to ensure the efficiency of the programme.

The transport sector and the energy sector generally considered that national CI should be outside the scope of EPCIP.

The IT sector was divided on this issue with one response recommending that NCI remains outside of EPCIP and a second response feeling that NCI should be addressed by the EPCIP framework, but not by specific regulations.

The tank storage industry felt that EPCIP should not deal with NCI.

The security industry felt that NCI should preferable be integrated in EPCIP.

The water and chemical industries did not provide an answer to this issue.

National CIP programmes (question 7.2)

The EPCIP Green Paper proposed that each Member State develop a National CIP Programme for its NCI based on the common EPCIP framework.

The single response from the transport sector which addressed this issue stated that each Member State should develop such national programmes addressing ECI within the EPCIP framework, and NCI autonomously.

The energy sector seemed to favour basing EPCIP on national programmes rather than national programmes on EPCIP.

The IT sector and the security sector favoured having each Member State adopt a National CIP Programme.

The water, tank storage and chemical industries did not provide an answer to this issue.

Single overseeing body (question 7.3)

The transport sector felt that it should be the Member States who are responsible for designating and managing NCI. The industry also saw added value in having a single coordinating body dealing with CIP issues.

The energy sector and the IT sector generally felt that this issue should be left to each Member State to decide.

The security sector thought that a single coordination body should be created in each Member State.

The water, tank storage and chemical industries did not provide an answer to this issue.

Implementing steps for NCI (question 7.4)

The transport sector did not provide a clear line concerning the implementing steps for NCI. One response reiterated the position that NCI should be outside of EPCIP. Another response felt that the steps were acceptable.

The IT sector limited itself to stating the implementation should be done under the authority of the national CIP body.

The security industry generally supported the list of steps but underlined that private partners should be involved more in the process.

The energy, water, tank storage and chemical industries did not provide a clear view on this issue.

Responsibilities of CI owners/operators(question 8.1)

The general business position was that the list of proposed responsibilities is unclear and may be too burdensome.

The transport sector was divided on this issue. One response clearly stated that the list is acceptable and found the OSP concept useful. Another response underlined that the EPCIP should have at its disposal the necessary financial measure to support the owners/operators.

The energy sector was generally positive about the list of responsibilities although it underlined that the private sector must be involved in discussing this issue.

The IT sector felt that owners/operators should be required to notify the relevant authorities about the fact that they may possess CI.

The security industry offered general comments on this issue.

The energy, water, tank storage and chemical industries did not provide a clear view on this issue.

Dialogue with CI owners/operators(question 8.2)

All industry associations underlined the need for dialogue with CI owners/operators during the development and implementation of EPCIP. Most felt that it should be the associations which represent the relevant sectors in the discussions.

The critical infrastructure warning information network (CIWIN) (question 9.1)

The transport sector supported the idea of creating CIWIN, but different opinions were expressed concerning its structure. One response supported the idea of CIWIN being limited to a rapid-alert network as relevant discussion fora already exist. Another response saw CIWIN as a multilayered communication system composed of two pillars.

The energy sector also supported the idea of CIWIN functioning only as a rapid alert system with the owners/operator being connected to the network.

The IT sector was of the opinion that CIWIN should first become a platform for the exchange of idea and best practices, to later develop into a RAS. Owners/operators should be connected to the system.

The security industry felt that CIWIN should be a 2-pillar system and that owners/operators should also be connected.

The energy, water, tank storage and chemical industries did not provide a clear view on this issue.

Common methodologies (question 9.2)

The single response from transport sector on this issue limited itself to stating that the harmonization of alert levels would be a difficult task.

The energy sector saw added value in harmonizing alert levels but admitted that this would be a very difficult task.

The IT sector and the security industry commented that the development of common methodologies and a harmonization of alert levels would be necessary.

The water, tank storage and chemical industries did not provide a clear view on this issue.

Funding (question 9.3)

The industry associations commenting on this issue underlined that a considerable amount of funding would be needed for EPCIP to be a success. The associations did not provide estimates of the costs involved. Most replies were positive concerning the availability of funds for research purposes.

Evaluation and monitoring (question 9.3)

Most industry associations commenting on this issue felt that some sort of evaluation mechanism would be needed. The transport sector generally accepted the proposed methods. One response from the energy sector expressed concern over the possibility of imposing penalties.