000017/EU XXIV.GP
Eingelangt am 28/10/08

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 27.10.2008
SEC(2008)2701

COMMISSION STAFF WORKING DOCUMENT

Accompanying document to the

Proposal for a
COUNCIL DECISION
on creating a Critical Infrastructure Warning Information Network (CIWIN)
{COM(2008) 676 final}
{SEC(2008) 2702}

IMPACT ASSESSMENT

EN

***

TABLE OF CONTENTS

1. Procedural issues and consultation of interested parties 4

1.1. Organisation and timing 4

1.2. The Impact Assessment Board 6

1.3. Consultation and expertise 6

1.4. Influence of the Green Paper responses on the CIWIN proposal 7

1.5. Influence of the CIWIN Study on the CIWIN proposal 8

2. Problem definition 10

2.1. Description of the problem 10

2.2. Parties affected by the problem 11

2.3. Baseline scenario 12

2.4. EU's right to act 13

3. Objectives 15

4. Policy options 17

5. Analysis of impacts of general policy 19

5.1. Option 1: No policy option 19

5.1.1. Financial impacts on public budgets 19

5.1.2. Economic impacts: 20

5.1.3. Environmental impacts 20

5.1.4. Social impacts 20

5.2. Option 2: CIWIN as an upgrade of existing RAS 21

5.2.1. Financial impacts on public budgets: 21

5.2.2. Economic impacts: 22

5.2.3. Environmental impacts 22

5.2.4. Social impacts 22

5.3. Option 3: CIWIN as an open platform for the (unsecured) exchange of CIP related information 23

5.3.1. Financial impacts on public budgets: 23

5.3.2. Economic impacts: ... 24

5.3.3. Environmental impacts ... 24

5.3.4. Social impacts ... 24

5.4. Option 4: CIWIN as a secure voluntary/opt-in multi-level communication/alert system composed of two distinct functions: a rapid alert system and an electronic forum for the exchange of CIP ideas and best practices ... 25

5.4.1. Financial impacts on public budgets: ... 25

5.4.2. Economic impacts: ... 27

5.4.3. Environmental impacts ... 27

5.4.4. Social impacts ... 27

5.5. Option 5: CIWIN as a compulsory multi-level communication/alert system composed of two distinct functions: a rapid alert system and an electronic forum for the exchange of CIP ideas and best practices ... 28

5.5.1. Social impacts ... 29

6. Comparing the options as to the general approach ... 30

Table of symbols ... 30

Summary table 1 – Negative impacts ... 30

Summary table 2 – benefits ... 31

Advantages and drawbacks of the policy options ... 32

7. Preferred policy option ... 34

7.1. Respect for fundamental rights ... 36

7.2. Costs of preferred option ... 36

8. Monitoring and evaluation ... 38

8.1. Core indicators of progress ... 38

8.2. Possible monitoring and evaluation arrangements ... 38

Annex I ... 39

Annex II ... 55

Annex III ... 58

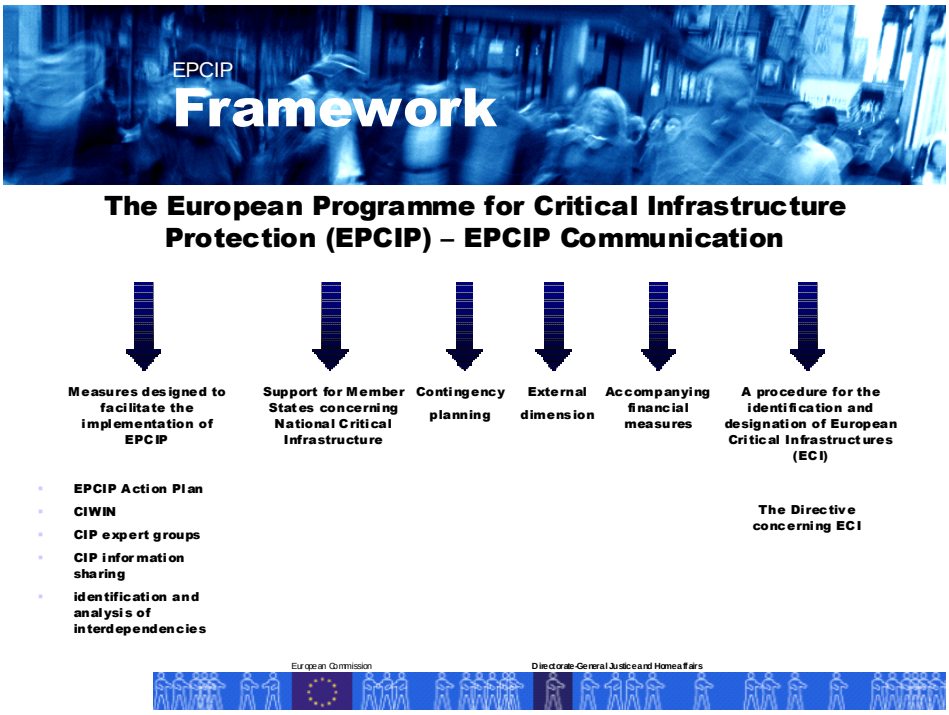
Annex IV ... 96

1. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

1.1. Organisation and timing

The Critical Infrastructure Warning Information Network (CIWIN) initiative is part of the European Programme for Critical Infrastructure Protection (EPCIP),[1] and it refers more specifically to the information sharing process between EU Member States and an information technology system to support that process.

Table 1: The EPCIP Framework



The European Council of June 2004 asked the Commission to prepare an overall strategy to protect critical infrastructure. The Commission adopted on 20 October 2004 a Communication on Critical Infrastructure Protection (CIP) in the Fight against Terrorism which put forward suggestions on what would enhance European prevention, preparedness and response to terrorist attacks involving critical infrastructures. The Council conclusions on "Prevention, Preparedness and Response to Terrorist Attacks" and the "EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks" adopted by Council in December 2004 endorsed the

[1] The term critical infrastructure is defined by the proposal for a Directive on the identification and designation of European Critical Infrastructure as "*"Critical Infrastructure" means those assets, systems or parts thereof located in the EU Member States which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions".*

intention of the Commission to propose an European Programme for Critical Infrastructure Protection and agreed to the set-up by the Commission of CIWIN.

In November 2005, the Commission adopted a Green Paper on EPCIP which provides policy options on how the Commission could establish EPCIP and CIWIN.

In December 2006, the Commission proposed a Directive on the identification and designation of European Critical Infrastructure (ECI) and the assessment of the need to improve their protection.[2] At the same time, the Commission launched a Communication on the EPCIP.[3] Together, these documents set out the framework for infrastructure protection in the EU. The Communication sets forth the horizontal framework for the protection of critical infrastructures in the EU. This framework is among others composed of measures designed to facilitate the implementation of EPCIP including CIWIN.

Relevant work has been taken forward through the CIP sub-group of the Inter-service 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. The group meets on average twice a year, and has regular e-mail exchanges.

EPCIP is based on an all-hazards approach, while recognising the threat from terrorism as a priority. The EPCIP framework consists of:

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

- Measures designed to facilitate the implementation of EPCIP including an EPCIP Action Plan, the Critical Infrastructure Warning Information Network (CIWIN) and the use of CIP expert groups at EU level, CIP information sharing processes and the identification and analysis of interdependencies.

- Support for Member States concerning National Critical Infrastructures (NCI) which may optionally be used by a particular Member State.

- Contingency planning.

- An external dimension.

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

---

2 COM (2006) 787 final.

3 COM (2006) 786 final.

Within the EPCIP package, it is the Communication that specifically refers to the creation of CIWIN. It states that CIWIN will be set up through a separate Commission proposal and will provide a platform for the exchange of best practices in a secure manner:

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

Therefore, CIWIN can only be understood as one of the measures within in the framework of EPCIP, and as bringing into operation the activities that have already been agreed upon. The set-up of the CIWIN system for the exchange of CIP related information needs to be viewed and discussed within the framework of EPCIP, as one of many steps that can improve and facilitate the sharing of information on the EU level.

1.2. The Impact Assessment Board

On 6 June 2008, the Impact Assessment Board of the European Commission delivered an opinion regarding a preliminary version of this Impact Assessment report. The Board stated that the IA report would be usefully complemented by including a description of the existing COM rapid alert systems that deal with alerting EU Member States.

The Board further stated that:

- The baseline scenario should be further developed and the value added of the CIWIN initiative better highlighted.
- The document should analyse the uptake of this initiative by the Member States.

The present version of the Impact Assessment report has been revised, with a view to taking these recommendations into account. Additional information and modifications have been introduced to this end in all relevant sections.

1.3. Consultation and expertise

All relevant stakeholders have been consulted on CIWIN through and within the consultation on EPCIP. This has been done through:

- The EPCIP Green Paper adopted on 17 November 2005 with the consultation period ending on 15 January 2006.[4] 22 Member States provided official responses to the consultation. Around 100 private sector representatives also provided comments to

[4] COM (2005) 576 final.

the Green Paper. The responses were generally supportive of the idea of creating CIWIN.[5]

- A number of informal meetings of Member States' CIP Contact Points which the Commission hosted (December 2005; February 2006; December 2006; November 2007, February 2008; March 2008).

- Study on the creation of a Critical Infrastructure Warning Information Network (CIWIN), concluded in January 2008 by an External contractor: Unisys. As part of the study the external contractor conducted interviews on CIWIN in all of the 27 Member States who responded to the requests.[6]

- Informal meetings with private sector representatives. Numerous informal meetings were held with representatives of particular private businesses as well as with industry associations.

CIWIN has been chosen as the name for this support for the CIP information sharing processes between the Member States. Since the end of 2006, work has been undertaken to shape CIWIN according to the purposes and the audience it will serve.

Through a consultation of the main actors to be involved in CIWIN, the EU Member States and the European Commission, CIWIN has moved from a broad outline to a functional prototype system.

1.4. Influence of the Green Paper responses on the CIWIN proposal

While the Green paper on EPCIP has been wider in scope, and consulted relevant stakeholders on many aspects of EPCIP (e.g. goal and key principles of EPCIP, implementing steps, etc), part of it focused also on CIWIN.[7]

The responses received to the EPCIP Green Paper and ongoing discussions with all stakeholders have had a major impact in shaping the proposal for CIWIN. In general, Member States did not have a uniform view concerning the setting up of the CIWIN network. Some Member States supported the setting up of CIWIN as a multi-level communication/alert system composed of two distinct functions: a rapid alert system and an electronic forum for the exchange of CIP ideas and best practices. A number of Member States however favoured limiting CIWIN to a forum for the exchange of CIP ideas and best practices; or to a rapid alert system (RAS) linking MS with the Commission. At the time of the consultation, two Member States were against the setting up of the CIWIN system.

In reference to the issue of connecting critical infrastructure owners/operators to CIWIN, the majority of Member States favoured linking critical infrastructure owners/operators to CIWIN.

---

5 The green paper (without annexes) as well as the summary report concerning the responses received from the Member States to the EPCIP Green Paper (only the relevant part referring to CIWIN) consultation are included in Annex I and II.

6 Relevant excerpts for the Study can be found in Annex III.

7 For more detailed information on the results of the consultation, see Annex II.

Nevertheless, some gave their support for connecting critical infrastructure owners/operators to CIWIN only if CIWIN was limited to a forum for the exchange of best practices. Moreover, a number of Member States underlined that different access levels should be given to different types of organisations connected to the network. Five Member States were against the idea of connecting CI owners/operators to CIWIN. Three Member States did not provider comments concerning this issue.

A major aspect that has been stressed within the consultation process has been the sensitivity and confidentiality of critical infrastructure related information.

When developing the policy options described in Section 5, all the different views received have been taken into consideration and weighted against financial, economic and social impacts. Where possible, a compromise solution has been developed.

1.5. Influence of the CIWIN Study on the CIWIN proposal

The results of the green paper consultation left some uncertainties concerning CIWIN, and the possibilities of creating an IT platform that would be able to compromise between different views on CIWIN. Therefore, a more detailed analysis on possible solutions, and existing practices and structures in Member States, was needed.

In March 2006 DG JLS awarded a contract that included a study into the possibility of the establishment of CIWIN. The objective of this study was to collect information on best practices for CIP and to undertake interviews with experts in Member States in order to define the requirements of CIWIN, both as an exchange network and a rapid alert system, taking into account the infrastructures and networks that exist at the national and international levels.

The CIWIN project was also aimed at studying the establishment of a common platform for the exchange of information relevant to CIP. The concrete objectives of the study were to:

- Establish an overview of and assess the existing national CIP networks and systems and the Member States' needs regarding CIWIN;
- Based on the results of the analysis, draw up and propose the requirements of the CIWIN system, at a central level and at the level of its interaction with the Member States;
- Create an implementation plan for CIWIN in order to enable the Commission to estimate the cost and effort required
- The demonstration of the feasibility of CIWIN as proposed, by creating a prototype for the two main target functions: a network for the exchange of CIP best practices and information, including contacts data, and an option for a rapid alert system.

When preparing the impact assessment, weighting different policy options, the results of the study and Member States' opinions and arguments were fully taken into consideration and influenced the approach taken significantly.[8]

[8] Excerpts from the CIWIN study can be found in Annex III.

2. PROBLEM DEFINITION

What needs to be stressed initially is that CIWIN represents only one of EPCIP's implementing steps, and only one of the initiatives that contribute to better information sharing and exchange of relevant best practices. Other initiatives that run in parallel to CIWIN are for example regular meeting with Member States in the framework of CIP Contact Points, the creation of CIP Expert Groups, etc. CIWIN should therefore not be considered as a separate initiative, but always and only within the context of the EPCIP package and other EPCIP implementation activities.

2.1. Description of the problem

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, financial services and transport systems, health services and the provision of safe drinking water and food is crucial to the functioning of the EU and its Member States. The destruction or disruption of infrastructure providing key services, on one hand, and inappropriate response to this kind of events, on the other hand, could entail *inter alia* the loss of lives, the loss of property and a collapse of public confidence in the EU.

There is a direct link between European interdisciplinary cooperation and national safety and security. In today's world of cross-border sector interdependencies both geographic cross-sector terms, Member State may offer services to other Member States or may have an impact on the provision of services in other Member States. There exists the risk of one Member State suffering because another has failed to adequately protect infrastructure on its territory.

A growing number of infrastructures are becoming increasingly European, which means that a purely national approach to dealing with them is insufficient. There is a clear need for addressing the broad range of threats that may touch Europe's critical infrastructure. Sectors such as IT, transport or energy simply underpin all the others.

In the case of such infrastructure, it is equally important for the Member States who are dependent on the service that infrastructure provides or may be influenced by that infrastructure, to have access to some of the relevant information that might concern it. 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,[9] which are not immediately and obviously interconnected. As such interconnectedness is insufficiently researched; this might certainly result in insufficient critical infrastructure protection and security of EU citizens.

Furthermore, the critical infrastructure present in the European Union is currently subjected to a varying puzzle of protective measures and obligations, without minimum standards being applied

[9] For example, a disruption of 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 Member States' authorities in particular those enabled by Information and Communications Technologies (ICTs).

horizontally. Some Member States are already far advanced in the process of identifying their national critical infrastructure, have imposed strong protection measures, and have a variety of practices and structures available to ensure its protection. Other Member States are only starting this process, and might benefit significantly by having access to relevant best practices such as for example risk assessment methodology. Therefore, another problem identified is insufficient co-operation, co-ordination and exchange of information between various CIP stakeholders in Europe. The problem can be identified in geographical (i.e. between Member States) and sectoral (i.e. between various CIP sectors) terms.

Addressing the exchange of information between Members States is a very complex area that requires a well-considered approach. It is important to prevent possible duplications of activities resulting from insufficient information on similar situations in other Member States, for example information on an already developed best practice in a specific Member State might avoid the cost of re-developing a similar practice in a different Member States.

Furthermore, fear of exchanging sensitive information is present among relevant stakeholders. One of the factors, contributing to such fear is that (1) the EU has not yet established an European CIP community, composed of actors willing and interested both in sharing information and experiences, as well as in consulting with each other in order to reach appropriate (common) standards for CIP in Europe; (2) stakeholders' fear of being obliged to share information they do not wish to share. In order to be able to exchange information efficiently, an environment of trust that allows all the necessary flexibility has to be established.

The problem

The main problems on which the solution should therefore focus, are:

- Insufficient protection of the EU critical infrastructure;
- Insufficient CIP co-operation between Member States;
- Difficult, and inefficient exchange of information on critical infrastructure between the Member States;
- Duplication of activities;
- Insufficient trust and willingness of stakeholders to exchange sensitive information.

2.2. Parties affected by the problem

The problem potentially affects all European citizens, inhabitants of the European Union, the Member States' governments and business, both directly and indirectly.

- *Citizens*. Insufficient security of EU citizens, including the potential loss of lives, the destruction of private property and the disruption of services is a major concern for the citizens. Event though the insufficient exchange of information and best practices between

critical infrastructure stakeholders does not affect European citizens directly, it certainly affects their security in an indirect way.

- *Business.* The existence of vulnerable infrastructure affects EU businesses by potentially destructing property and the disrupting services/shipments businesses rely on. Among others inefficient exchange if information on protection measures in other Member States or other sectors, or knowledge on examples of standard operator security plans, business owners/operators could result in higher economic costs for the development of practices as they might already exist elsewhere.

- *Governments.* Governments are affected by the existence of vulnerable infrastructure as they too are dependent on services provided by such infrastructure. Inefficient and unreliable access to experiences and practices in other Member States might prove costly to those member States who are currently at an early stage of their CIP plans or policies.

2.3. Baseline scenario

Without an EU approach to understanding interdependencies and security externalities, and sharing experiences and practices, i.e. the *status quo* scenario, private and public decision-makers would continue to have limited access to information on critical infrastructure protection activities and practices in the EU.

If the existing problem of insufficient information sharing would continue without horizontal actions at EU level, national critical infrastructure policies would continue to exist; however, those who are currently developing the same policies would not be able to benefit from access to relevant information. While it is clear that CIP is the responsibility of Member States, information exchange on best practices could avoid unnecessary duplication of efforts. The *status quo*, on the other hand, would certainly not enable EU Member States to learn from the mistakes or successes of others. In other words, Member States could not benefit from the already existing knowledge in other Member States and would have to invest national funds in acquiring knowledge that might actually already exist in another Member State. Furthermore, the *status quo* would deprive those Member States who wish to participate in the exchange of best practices and reinforce their dialogue of the possibility to do so in a secure and efficient environment. Member States' authorities would have no direct access to a platform containing relevant best practices (e.g. risk assessment methodologies), which might also be available (depending on the level of classification of the information) to representatives of industry sectors (owners and operators of critical infrastructure). By consequence, no policy option would result in some operators/owners of critical infrastructure not benefiting form an efficient transfer of knowledge already acquired in other sectors or by other owners and operators.

As most Member States see the need to address CIP issues at European level, and benefit from sharing information and exchanging alerts, an alternative solution to the exchange of information would have to be found. Without a European approach, such solution could be less transparent and could leave out many Member States.

Also in policy area development terms, the baseline line scenario would deprive EPCIP of a necessary implementation tool thus hindering achieving the underlying objective of improving

the protection of European critical infrastructure. This would ultimately deprive the EU Member States of the possibility to securely reinforce their CIP dialogue and share information within a coherent, secure and efficient framework (impacts of the baseline scenario are explained in section 5.1).

As regards the exchange of alerts on CIP, if the present situation was to continue, the EU would remain without a cross-sectoral alert IT tool. The Commission has developed over the years the operational capacity to assist in the response to a wide range of emergencies through several rapid alert systems (RAS), such as the CECIS (Common Emergency Communication and Information System), ECURIE (in the event of a radiological emergency), RAS-BICHAT (for biological and chemical attacks and threats), RAPEX (consumer health and safety - non-food aspects), RASFF (consumer health in relation to food and feed), EWRS (communicable diseases), EUROPHYT (phytosanitary network), SHIFT (health controls on imports of veterinary concern), TRACES (animal transportation) and ADNS (animal health).[10] Each of these RAS focuses on specific sectors, some of which correspond also to the CIP sectors. Nevertheless, none of the existing RAS at this moment provides a horizontal and cross-sectoral functionality that would be accessible to a wider range of stakeholders (relevant national CIP agencies and ministries etc) than just emergency services. Most of the RAS have a sectors specific character, and are directed to specialised services within the EU (e.g. health authorities). The interconnectedness of infrastructures within the EU as well as the existence of strong interdependencies between sectors (e.g. electricity networks and ICT sector) demonstrates that a horizontal approach to critical infrastructure protection is needed. Therefore, the EU would inevitably have to consider the horizontal and cross-sector approach to RAS in the EPCIP implementation phase. Solutions such as combining the existing RAS and ensuring their interoperability could be considered; nevertheless due to the technical difficulties of doing so, such a solution is costlier than the creation of a new RAS.

The status quo scenario would not have any direct impacts on the environment. Nevertheless, some indirect negative effects on environment, resulting from uncoordinated and thus inefficient exchange of alerts, could appear.

2.4. EU's right to act

Although several sectoral legal bases for CIP 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

[10] The Commission has also set-up an internal general rapid alert system (ARGUS) to link all specialised systems for emergencies.

- To promote the raising of the standard of living and quality of life

- To promote solidarity among Member States.

Furthermore, Article 308 of the Treaty stipulates that if action by the Community should prove necessary to attain, in the course of the operation of the common market, one of the objectives of the Community, and this Treaty has not provided the necessary powers, the Council shall, acting unanimously on a proposal from the Commission and after consulting the European Parliament, take the appropriate measures. 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.

Subsidiarity and proportionality principles

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 under its jurisdiction, an all-EU and cross-border platform for exchange of information that ensures that information is available to all Member States who might benefit from it, can certainly be implemented only at EU level. No Member State alone can ensure a pan-European exchange of information or the exchange of rapid alerts. It is therefore clear that working at EU level provides the added value of co-ordination of pieces of information that might already be available but are not shared with others. Only a European approach can ensure that Member States who wish to share and receive information are treated equally, that co-operation does not geographically discriminate member States, and that the information indeed reaches those who wish to receive it.

This proposal should also not go beyond what is necessary in order to achieve the underlying objectives of Member States co-operation in the field, especially with regard to the Member States' willingness to participate.

3. OBJECTIVES

As mentioned earlier, CIWIN has to be understood in the broader sense of EPCIP. Therefore, the general objective of CIWIN is to contribute to the improvement of the protection of critical infrastructure in the EU.

The specific objective of CIWIN is to enable co-ordination and co-operation concerning the information on the protection of critical infrastructure at EU level. Most importantly, it should ensure secure and structured exchange of information and thus allow its users to learn about best practices in other EU Member States in a quick and efficient way. Such an exchange would bring a considerable added value.

The concrete issue at hand which requires action at EU level is to facilitate the exchange of relevant information between Member States' authorities, and enable them to use the rapid alert system concerning CIP. Such system would be dependent upon - but at the same time would also contribute to - building trust among Member States.

In other words CIWIN's specific objective is to stimulate the development of appropriate measures aimed at facilitating an exchange of best practices as well as being a vehicle for transmission of immediate threats and alerts in a secure manner. The system should ensure that the right people have the right information at the right time.

The creation of CIWIN has already been envisaged in the Communication on a European Programme for CIP, and CIWIN itself as an IT tool is one of EPCIP's operational objectives. Nevertheless, operational (sub)objectives that CIWIN intends to achieve can be identified as follows:

- to provide an IT tool that will facilitate CIP co-operation between Member States;

- to offer an efficient and quick alternative to often time-consuming methods of searching for information, i.e. create a type of "one-stop-system" to obtain all relevant information on critical infrastructures in the EU;

- and to offer the possibility to Member States to communicate directly and upload information that they deem relevant.

Since some of the Member States would prefer to use only some of the functionalities that CIWIN offers, one of the main operational objectives is to identify a solution that would allow Member States an opt-in/opt-out possibility on certain aspects of the system.

Furthermore, trust needs to be the core principle on which CIWIN is to be based and be one of its main driving forces, based on the input received from all identified users: Member States governmental authorities, supervisory authorities, experts in CIP, the European Commission. Building trust should mainly be achieved by the creation of an effective European CIP community, composed of actors willing and interested both in sharing information and experiences, as well as in consulting with each other in order to reach appropriate (common) standards for CIP in Europe.

Trust can also be achieved by ensuring that the system used is adequately secure and that security itself is taken seriously, by providing the necessary procedures and tools for ensuring the level of security required by the users. Careful management of the provision of access rights to its users has to be one of the main elements contributing to the building of trust in both the CIWIN system and its user community. The "need to know" principle and an adequate protection of the information contained have to be at the basis of the granting of access to CIWIN.

Flexibility is another basic concept on which to build CIWIN. Taking into account the hybrid nature of the topics it is covering, the structure should be sufficiently flexible to cater for the needs of all the different critical infrastructure sectors identified under the European Programme for Critical Infrastructure Protection (11 sectors, 29 sub-sectors) and the users linked to it.

By endorsing the idea of the creation of CIWIN as a general support and facilitator for the information sharing process between the Member States, the need for and importance of a cross-sectoral approach as promoted by the EPCIP is generally accepted by the consulted Member States.

4. POLICY OPTIONS

The intention and agreement on the adoption of a separate proposal for the establishment of CIWIN has been already reached within the EPCIP package, more specifically by the Commission's Communication on the EPCIP. Following from that, a "No policy option" is difficult to envisage, nevertheless it is taken into consideration in the approaches outlined below. After extensive consultation with the Member States and CIP experts, 5 different policy options can be envisaged:

Option 1: No policy option.

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 (more information in section 2.3).

Option 2: CIWIN as an upgrade of existing RAS

Under this option, CIWIN's role would be to ensure the inter-operability of the existing RAS, and make them accessible to different services within the EU and ministries in Member States. This option would require both a functional revision of existing IT architecture and legislative modifications to their legal base. As such an option would contain rapid alert functionalities only. Under this option access to existing RAS would have to be broadened including CIP related stakeholders. Such a development would also depend on the support of the EU MS to such a solution.

Option 3: CIWIN as an open platform for the (unsecured) exchange of CIP related information

Under this option an IT tool that would be opened to the general public and would function as a regular internet site would be established. Such solution would certainly contribute to raising awareness on CIP in Europe and increase direct information exchange among the stakeholders. Nevertheless, as the owner of the information uploaded would never know who the final user of the information is, the information uploaded would be severely limited.

Option 4: CIWIN as a secure voluntary/opt-in multi-level communication/alert system composed of two distinct functions: a rapid alert system and an electronic forum for the exchange of CIP ideas and best practices

Under this option, CIWIN would be established as an IT tool that would be able to contain and transmit sensitive information, classified up to the level of UE RESTREINT.[11] The system would consist of two main functionalities: (1) a secure forum for the exchange of information, where strong emphasis would be given to the exchange of best practices, dialogue and the building of trust at EU level; (2) a rapid alert system for critical infrastructure. Member States would be free

[11] The information protection measures applicable are specified in the Decision 2001/844/EC.

to use the entire system, to choose between the functionalities offered or not to use the system at all.

Option 5: CIWIN as a compulsory multi-level communication/alert system composed of two distinct functions: a rapid alert system and an electronic forum for the exchange of CIP ideas and best practices

Under this option, CIWIN would be a compulsory system, where each Member State would be obliged to upload and update the relevant information regularly. The option would certainly prevent Member States from deciding not to share the information that might be useful to another Member States; however it is questionable whether such obligatory approach would contribute to building trust among Member States.. Furthermore, the approach may be contrary to the proportionality principle and could be rejected by Member States.

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 financial, economic and social context in comparison to the baseline scenario that is the no policy option .The likelihood of an impact is the probability that this impact will occur.

Table of symbols "-" for negative impacts and "+" for positive impacts	
Small magnitude	- / +
Medium magnitude	-- / ++
Significant magnitude	- - - / +++
Low likelihood	√
Medium likelihood	√√
High likelihood	√√√
Baseline	0

Only those areas of the financial, economic, environmental and social impacts that are relevant to the case are considered. It is also important to note that the outlined impacts take into consideration also the expected take up of MS for each of the policy options.

5.1. Option 1: No policy option

No policy option would deprive the EU Member States of the possibility to reinforce their dialogue and share information within a coherent, secure and efficient framework. As this policy option represents the baseline scenario, it is described in more details in section 2.3.

As this policy option represents the baseline scenario, it is important to stress that its present impacts represent the basic reference value to which other policy options are compared to and therefore the reference value of magnitude the of the impacts of Option 1 is always represented by 0.

5.1.1. Financial impacts on public budgets

Costs for Member States' budgets The likelihood of Option 1 having an impact on public authorities would be high. In this assessment 2 aspects, short-term (and direct impact), and long-term (and indirect impact) have to be considered.

As regards the short- term impacts, Member States would not be affected by the no policy option.

- Likelihood: 0

In case nothing would be done at EU level, Member States could not benefit from the already existing knowledge in other Member States and would have to invest national funds in acquiring knowledge that might actually already exist in another Member State. Furthermore due to interdependencies - not only sectoral, but also geographical - of European Critical Infrastructure, a solution or multiple solutions to exchange the information would have to be found. Such a not coordinated and inefficient approach can be expected to be costly.

- Likelihood: √√√

Costs for the EU budget. EU budget would not be affected by the no policy option.

- Likelihood: 0

5.1.2. Economic impacts:

Financial cost for sectors of industry affected. In case of a no policy option, representatives of industry sectors would have no direct access to best practices and efficient transfer of knowledge already acquired in other sectors or by other owners and operators would not be possible. By consequence, representatives of industry sectors would certainly encounter additional costs when acquiring knowledge in the field.

- Likelihood: √√

Innovation and research. Innovation and research is needed in order to improve the protection of critical infrastructure in Europe. Inefficient and not transparent exchange of information would hinder dissemination of relevant and potentially innovative approaches to for example methodologies to risk assessment, etc. Such an exchange of information could also be very varied in geographic terms.

- Likelihood: √

5.1.3. Environmental impacts

As an IT tool, CIWIN does not have any direct impact on the environment. However some indirect negative effects on the animal and plant health, food and feed safety, could appear.

- Likelihood: 0

5.1.4. Social impacts

Crime, terrorism and security. In the no policy option insufficient and inefficient exchange of e.g. alerts or information between Member States would persist. Taking into consideration growing interdependencies, the current difficult and not coordinated access to relevant information could have an influence on the security of critical infrastructure in Europe and thereby the general security and safety of its citizens as would not be ensured sufficiently.

- Likelihood: √√

Building trust among stakeholders. Option 1 would not facilitate any significant trust building at the EU level, as the contacts between all stakeholders involved in the CIP process would remain occasional and not coordinated.

- Likelihood: √√√

Improving the exchange of best practices. Option 1 would be unlikely to improve exchange of best practices and in particular improve their availability to all EU Member States.

5.2. Option 2: CIWIN as an upgrade of existing RAS

Among the possible CIWIN policy options, CIWIN as an upgrade of existing RAS is an option that would inter-connect all existing RAS in order to ensure a cross-sectoral alerts exchange. A solution where CIWIN would be a RAS only has been considered by the CIWIN study;[12] however it received very limited support from Member States.

5.2.1. Financial impacts on public budgets:

Impact on Member States' budgets. CIWIN as an upgrade of existing RAS would entail important direct costs on Member States' budgets on a short-term, as it would have to involve a revision of the administrative IT-systems that currently connects specific national authorities (e.g. sectoral ministries) to sectoral RAS as well as including CIP stakeholders in existing RAS. It would also require revisions of the legal bases involved. A considerable administrative effort would have to be made to define the most efficient system of doing so in each Member State.

- Magnitude impact on Member States' budgets: -
- Likelihood: √√√

Nevertheless, in comparison to a no-policy option, there might be long-tem benefits deriving form Option 2. This concerns especially the preventive role of the RAS, i.e. a timely alert might prevent the disruption or destruction of a specific critical infrastructure, thus avoiding the potential costs of such disruption or destruction form Member States budgets.

- Magnitude impact on Member States' budgets: +
- Likelihood: √√

Impact on the EU budget. The likelihood of Option 2 having a short-term impact on the EU budget would be high; and its magnitude medium. Option 2 would certainly involve a considerable technical effort of interlinking various RAS that are currently operating on different IT systems, and are also being maintained and administrated by a variety of external contractors. Defining the exact cost of the interoperability of different RAS alone necessitates a specific detailed study, which would be already costly on its own but can certainly be expected to be high.

[12] See Annex III.

– Magnitude of the impact on the EU budget: --

– Likelihood: √√√

5.2.2. Economic impacts:

Financial cost for sectors of industry affected. As mentioned earlier (point 5.1.2.), sectors of industry will not incur any direct and financial costs from the implementation of CIWIN in any of its forms. In CIWIN as an upgrade of existing RAS an exchange of information would not occur, the co-operation would be limited to the exchange of alerts, only.

– Magnitude of impact on financial costs for sectors of industry affected: 0

– Likelihood: 0

Innovation and research. CIWIN as an upgrade of existing RAS would not in any way affect innovation and research.

– Magnitude of the impact on innovation and research: 0

– Likelihood: 0

5.2.3. Environmental impacts

CIWIN as a system for the exchange of alerts could only indirectly (e.g. by exchanging an alert that would prevent the disruption of destruction of a specific critical infrastructure – for example a chemical plant) represent a beneficial impact on the environment.

– Magnitude of the impact on environment: +

– Likelihood: √

5.2.4. Social impacts

Crime, terrorism and security. The exchange of CIP alerts between the Member States would certainly help increase the security and safety of EU citizens. However, due to the limited number of information exchanged (only alerts and not best practices), the magnitude of the positive impact would be small.

– Magnitude of the impact on increasing EU security: +

– Likelihood: √√

Building trust among stakeholders. By regular exchange of CIP alerts among Member States, their co-operation on CIP matters would certainly become more regular than in the No policy option. Thus, Option 2 would contribute to the building of trust among the stakeholders; however the scale and likelihood of the impact would be small as the scope of the information exchanged would be limited to alerts.

– Magnitude of the impact on building trust among stakeholders: +

– Likelihood: √

Improving the exchange of best practices. As the contacts among Member States would be limited to the exchange of alerts only, Option 2 would not in any way affect the exchange of best practices.

- Magnitude of the impact on improving the exchange of best practices: 0
- Likelihood: 0

5.3. Option 3: CIWIN as an open platform for the (unsecured) exchange of CIP related information

Among the possible CIWIN policy options, CIWIN as an open platform for the (unsecured) exchange of CIP information received only limited support among the Member States, during the visits organised by the contractor.[13] Among the most often stated arguments in favour of such option was that the vast majority of the information to be exchanged does not require any particular measures to limit its distribution as this is publicly available information or information which is harmless.

5.3.1. Financial impacts on public budgets:

Impact on Member States' budgets. CIWIN as an open platform would bring small direct cost on Member States, limited to the labour costs of the officials assigned to administer the Member States' part of CIWIN. The likelihood of this option having a cost for Member States would be high and the magnitude of the impact small.

- Magnitude of the short term impact on Member States' budgets: -
- Likelihood: √√√

Nevertheless, the long-term benefits of such a solution, that might outweigh the short term costs, have to be considered. CIWIN as an open platform would include information such as best practices on Standard Operator Security plans, risk assessment methodologies etc, Member States budgets might benefit from having already developed knowledge in Europe ready and available. Nevertheless, due to the general availability of such information, the holder of relevant CIP information (which is generally considered as sensitive) might decide not to make it publicly available and therefore not share it. As a consequence the likelihood of this option providing such a benefit to Member States is low.

- Magnitude of the long term impact on Member States' budgets: ++
- Likelihood: √

Impact on the EU budget. The likelihood of Option 3 having an impact on the EU budget would be medium; however its magnitude would be small. The European Commission already developed a CIWIN prototype for the cost of 250,000 EUR (the prototype has been developed by

[13] See Annex III.

an external contractor), which focused on the idea of CIWIN as a system for a secure exchange of information

- Magnitude of the impact on the EU budget: -
- Likelihood: √√√

5.3.2. Economic impacts:

Financial cost for sectors of industry affected. As mentioned earlier, sectors of industry will not incur any direct and financial costs form the implementation of CIWIN in any of its forms. Nevertheless, by establishing CIWIN, relevant stakeholders, including owners and operators of critical infrastructure would have a more direct knowledge on best practices that could also be available in a single place. Nevertheless, in case of CIWIN being an open platform, the likelihood of the uploaded information having significant added value and going beyond the information that can already be found, is low.

- Magnitude of impact on financial costs for sectors of industry affected: +
- Likelihood: √

Innovation and research. Innovation and research is needed in order to improve the protection of critical infrastructure in Europe. Introducing CIWIN as an IT tool for the exchange of information can certainly facilitate the dissemination of relevant and potentially innovative approaches to; for example, improve risk assessment methodologies or even the development of new protection technologies. As the EU is already promoting research in this area (through Specific Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related Risks for the Period 2007-2013"), and considering the nature of information its owners would be willing to share in the publicly available environment, impacts would be limited.

- Magnitude of the impact on innovation and research: +
- Likelihood: √√

5.3.3. Environmental impacts

CIWIN as an open platform for the exchange of information is not likely to have any even indirect, impact on the environment. Due to the fact that such an option would not allow the possibility to exchange classified information or alerts, it is highly unlikely that a better organisation of already available information would change the current situation.

- Magnitude of the impact on environment: 0
- Likelihood: 0

5.3.4. Social impacts

Crime, terrorism and security. The exchange of information on CIP policies, practices in the Member States would help increase the security and safety of EU citizens. However, due to the open nature of the platform and the type of information exchanged (only non-classified

information would be available), the solution would not necessarily bring significant added value to those who are in charge of protection measures of critical infrastructure. Furthermore, having an open platform would also mean that Option 3 would not include the system for exchanging alerts as a functionality of the system. Therefore, the likelihood of Option 3 having an impact on EU security is medium and the magnitude of the impact would be low.

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

Building trust among stakeholders. Option 3 would not contribute significantly to the building of trust among the stakeholders because the information exchanged would be non – classified, and the amount of valuable sensitive information that could be shared would be very limited.

- Magnitude of the impact on building trust among stakeholders: +
- Likelihood: √

Improving the exchange of best practices. The adoption of Option 3 would improve the exchange of best practices, but in only to a limited extent. Its biggest added value would be better co-ordination and more transparency to the process, as it would collect all relevant information in one single place. Nevertheless the magnitude of the impact would be quite small, because the information that stakeholders would be willing to exchange in an open forum would be limited.

- Magnitude of the impact on improving the exchange of best practices: +
- Likelihood: √√

5.4. Option 4: CIWIN as a secure voluntary/opt-in multi-level communication/alert system composed of two distinct functions: a rapid alert system and an electronic forum for the exchange of CIP ideas and best practices

Among the possible CIWIN policy options, Option 4 received the most support among Member States. The main advantages of the option would be that CIP information is considered sensitive, even if it is not formally classified. Contributors wish to restrict those who may receive their information to a limited and trusted group of users. Furthermore, in comparison to Option 3 (and due to the level of protection of the information exchanged), this option would allow the development of an additional functionality: a rapid alert system.

5.4.1. Financial impacts on public budgets:

Impact on Member States' budgets. The short term and direct costs of establishing CIWIN as a platform for a secure exchange of information are low and consist principally of the cost of providing dedicated PC terminals in suitably secure locations that are connected to the S-TESTA network.[14] The cost of providing the S-TESTA network to all Member States is already covered

[14] Trans European Services for Telematics between Administrations (TESTA) is a European Community's own private, IP-based network offering a telecommunications interconnection platform between European public administrations. For more information on the network: European Commission, 'TESTA: Trans European

by Community budgets. There may be additional cost for Member States where the department accessing CIWIN does not currently have local S-TESTA access; however this is expected to be the case for very few Member States, and the additional cost to provide such access is low. There will also be certain local training and support costs, which are inherent in using any new IT system, however the number of users is relatively limited, and the complexity of the interface is considered low.

- Magnitude of the short term impact on Member States' budgets: -
- Likelihood: √√√

Long term benefits for Member States are expected from having direct access to information that might not be otherwise easily available. As a considerable number of Member States is currently implementing national CIP programmes, having access to such information would be expected to contribute significantly to the avoidance of duplication and therefore to reduce the individual costs of developing methods and practices that exist in other Member States.

- Magnitude of the long term impact on Member States' budgets: ++
- Likelihood: √√√

Impact on the EU budget. The likelihood of Option 4 having an impact on the EU budget would be high; however its magnitude would be small. The European Commission already developed a CIWIN prototype for the cost of 250,000 EUR (the prototype has been developed by an external contractor: UNYSIS). To turn the prototype into a proper functional system, another 500.000 EUR shall be spent under the Specific Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related Risks for the Period 2007-2013" in 2008. An additional 400.000 EUR shall be spent in 2009 for the necessary technical support to security accreditation, maintenance, the provision of a helpdesk and training of Member States' authorities[15]. The implementation of appropriate business continuity and disaster recovery measures, providing a helpdesk, support and system administration will also have an associated cost. The Commission will also need to ensure readiness for the rapid alert functionality through organising exercises and maintaining appropriate procedures. There will also be effort required in obtaining and maintaining accreditation to RESTREINT UE.

The annual costs of support and maintenance of the system are expected to be approximately 250,000€/year. As regards the human resources aspect, the system is expected to require one half time AD official and one half time AST officials.

- Magnitude of the impact on the costs for the EU budget: -
- Likelihood: √√√

Services for Telematics between Administrations', April 2005, <http://europa.eu.int/idabc/en/document/2097>.

[15] The envisaged costs are based on a financial analysis and comparison of similar Commission IT-systems (rapid alert systems).

*5.4.2. **Economic impacts:***

Financial cost for sectors of industry affected. As already mentioned, industry sectors will not incur any direct financial costs form the implementation of the CIWIN in any of its forms. By establishing CIWIN as a platform for a secure exchange of information they also will not have direct access to the information contained in CIWIN. Therefore, the advantages of such information for the private sector will be limited by their classification and the distribution of relevant information will depend upon the relevant Member States authorities' willingness to distribute it through appropriate national channels. Nevertheless, it can be assumed that relevant information that might not need to be classified, e.g. certain best practices, will be distributed, therefore meaning that sectors might benefit from the knowledge already acquired in other sectors.

- Magnitude of impact on financial costs for sectors of industry affected: ++
- Likelihood: √√

Innovation and research. While in theory innovation and research benefits more from the general availability of the information, the added value of such information is decreased by the nature of the information available (i.e. only non-classified information). By introducing CIWIN as a secure system for the exchange of information, the likelihood of Member States having access to relevant information that might actually bring added value, increases. This can, for example, include the development of improved risk assessment methodologies or even the development of new protection technologies. As already mentioned, the EU is already financing such research with the Specific Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related Risks for the Period 2007-2013", which means that the contribution of this option to research and innovation is limited.

- Magnitude of the impact on innovation and research: +
- Likelihood: √√

5.4.3. Environmental impacts

CIWIN as a secure voluntary/opt-in multi-level communication/alert system could only indirectly (e.g. by exchanging an alert that would prevent the disruption of destruction of a specific critical infrastructure or a best practice that could help increase the security measures – for example in a chemical plant) represent a beneficial impact on the environment.

- Magnitude of the impact on environment: +
- Likelihood: √

*5.4.4. **Social impacts***

Crime, terrorism and security. The likelihood of Option 4 having an impact on EU security and the safety of its citizens is medium to high. CIWIN provides a platform where the information and alerts can be exchanged within a surrounding of trust. Ideally, such practice could in the long term develop a relationship between Member States where they would be willing to share information that might prove important not only from a national perspective, but also from an EU

perspective. A rapid alert system would allow the rapid distribution of information regarding a threat or an event (first and subsequent messages) to the relevant receivers with the purpose to allow the receivers to take well-founded time-sensitive actions and/or decisions. The likelihood of CIWIN contributing to this is medium, mostly due to the fact that the system would be an opt-in one.

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

Building trust among stakeholders. Building trust among all stakeholders would certainly be best served by an option where the information and alerts can be exchanged willingly and in a secure environment, and where the final user of the information is known in advance by those who upload specific information. Through time and through this option, CIWIN should prove one of the most important instruments of increasing trust among Member States, and thus their willingness to share relevant information and alerts.

- Magnitude of the impact on building trust among stakeholders: +++
- Likelihood: √√√

Improving the exchange of best practices. The exchange of best practices is actually one of the main purposes of CIWIN. While specific practices might not necessarily be classified, some certainly could. And while an open platform would result in a wider availability of such best practices, the result might also be the lack of willingness to share such information indiscriminately. Hence, providing a secure environment for the exchange of information and alerts increases the chances of increasing the quantity and quality of available information. The information that does not need to be classified can still be made available to alternative and appropriate national or EU channels (e.g. Expert group meetings at EU level)

- Magnitude of the impact on improving the exchange of best practices: +++
- Likelihood: √√√

5.5. Option 5: CIWIN as a compulsory multi-level communication/alert system composed of two distinct functions: a rapid alert system and an electronic forum for the exchange of CIP ideas and best practices

When considering CIWIN as a compulsory option, it is necessary to mention that the majority of variables such as for example cost for national or EU budgets, benefits for innovation, environmental impacts etc. remain unchanged in comparison to Option 4, and are thus not addressed explicitly.

The only changes refer to social impacts of Option 5, where it is clearer that the positive effects for security might be wider (this only in case of some of the Member States deciding not to use CIWIN as an tool for the exchange of information under Option 4), if it would be compulsory for all Member States to use the system.

5.5.1. Social impacts

Crime, terrorism and security. Exchanging relevant information alerts would certainly contribute to increasing the security in the EU and the safety of EU citizens. The likelihood of CIWIN contributing to the increase of security in the EU if all Member States participate in the system is high.

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

Building trust among stakeholders. It is questionable whether a system of obligations would actually contribute to building trust among the relevant stakeholders or have actually the opposite effect. In an environment, such as CIP policy, where not every activity can be regulated, some activities that are important for the security within the EU remain on a voluntary basis. The higher the level of trust between Member States, the higher the probability that the information on practices will be shared an exchanged voluntarily among Member States.

- Magnitude of the impact on building trust among stakeholders: ++
- Likelihood: √√

6. COMPARING THE OPTIONS AS TO THE GENERAL APPROACH

Table of symbols

Table of symbols distinguishes "-" for negative impacts and "+" for positive impacts	
Small magnitude	- / +
Medium magnitude	-- / ++
Significant magnitude	- - - / +++
Low likelihood	√
Medium likelihood	√√
High likelihood	√√√
Baseline	0

Summary table 1 – Negative impacts

Negative impacts	Option 1 – No policy option	Option 2 – Upgrade of existing RAS	Option 3 –open platform for the (unsecured) exchange of information	Option 4 – secure and opt-in multi-level system	Option 5 – secure and a compulsory multi-level system
Financial impacts on public budgets					
Impacts on Member States' budgets	Short term 0 0	Short term - √√√	Short term - √√√	Short term: - √√√	Short term: - √√√
Impacts on the EU budget	0 0	-- √√√	- √√√	- √√√	- √√√
Economic impacts					
Financial cost for sectors of industry affected	0 √√	/	/	/	/
Innovation and research	0 √	/	/	/	/
Environmental impacts					
Environmental impacts	0 0	/	/	/	/
Social impacts					
Crime,	0	/	/	/	/

terrorism and security	√√				
Building trust among stakeholders	0 √√√	/	/	/	/
Improving the exchange of best practices	0 √√√	/	/	/	/

As it is evident from the above table, the negative impacts of the three policy options compared against Option 1 are of small magnitude.

Summary table 2 – benefits

Positive impacts	Option 1 – No policy option	Option 2 – CIWIN as an upgrade of existing RAS	Option 3 – open platform for the (unsecured) exchange of information	Option 4 – secure and opt-in multi-level system	Option 5 – secure and a compulsory multi-level system
Financial impacts on public budgets					
Impacts on Member States' budgets	Long term 0 √√√	Long term + √√	Long term ++ √√	Long term ++ √√	Long term ++ √√
Impacts on the EU budget	0 0	Long term 0 0	/	/	/
Economic impacts					
Financial benefits for sectors of industry affected	0 √√	/	+ √	++ √√	++ √√
Innovation and research	0 √	/	+ √√	+ √√	+ √√
Environmental impacts					
Environmental impacts	0 0	+ √	0 0	+ √	+ √
Social impacts					
Crime, terrorism and security	0 √√	+ √√	+ √√	++ √√	++ √√√
Building trust among stakeholders	0 √√√	+ √	+ √	+++ √√√	++ √√
Improving the	0	0	+	+++	++

exchange of best practices	√√√	0	√√	√√√	√√

When comparing the 4 options to Option 1, Option 4 – CIWIN as a secure voluntary/opt-in multi-level communication/alert system composed of two distinct functions: a rapid alert system and an electronic forum for the exchange of CIP ideas and best practices - shows to be the one where the benefits are the clearest. The likelihood of Option 5 - CIWIN as a compulsory multi-level communication/alert system composed of two distinct functions: a rapid alert system and an electronic forum for the exchange of CIP ideas and best practices – having positive impacts on security in the EU is higher then in Option 4. Nevertheless, when speaking about other social impacts (i.e. building trust among stakeholders and improving the exchange of best practices), the magnitude and likelihood of Option 4 benefits exceeds that of Option 5.

Advantages and drawbacks of the policy options

Policy options	Advantages	Drawbacks
Option 1: no policy change	No additional legislative proposal; Member States remain completely free to address CIP issues as they see fit	The dialogue and information sharing between member States would remain the same. There would not exist any coherent, secure and efficient IT system to exchange CIP information in Europe. No impact on improving EU security. No assurances that all relevant stakeholders in Europe have access to relevant CIP information.
Option 2: upgrade of existing RAS	Existing RAS would be upgraded and would enable horizontal exchange of alerts with regard to critical infrastructure.	High costs of ensuring the inter-operability of existing RAS The option would not allow the exchange of information and best practices. In order to meet expectations of majority of Member States, a new platform for the exchange of information would have to be established entailing additional effort.
Option 3: open platform for the (unsecured) exchange of information	Wide access to CIP information. The private sector would have the possibility to contribute to the platform directly. While the information included in the system is already publicly available, CIWIN would offer efficient, co-ordinated and easy	The information included in the system will be limited to non classified information only. As such information is already available; the added value of such option is limited. No possibilities to exchange alerts.

	access to it.	
Option 4: secure and opt-in multi-level system	The system would offer a secure environment for the exchange of information and contribute significantly to building trust among stakeholders. The information included will go beyond what is already publicly available. The system would allow exchanging alerts. CIWIN would offer an efficient, easy to use IT system. CIWIN would contribute to increasing security in the EU.	The stakeholders from the private sector would not have direct access to CIWIN. The success of the system will depend on the member States' willingness to use it.
Option 5: secure and a compulsory multi-level system	All member States would be participating in the system. The information included will go beyond what is already publicly available. The system would allow exchanging alerts. CIWIN would offer an efficient, easy to use IT system. CIWIN would contribute in increasing security in the EU.	Member States would not support the proposal. A system of obligations might not contribute to trust building and would backfire. The system might go contrary to the principle of proportionality.

7. PREFERRED POLICY OPTION

The analysis of the five 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 5) could bring distinct benefits, but also a number of drawbacks.

Nevertheless, when weighting the benefits and drawbacks of all options, Option 4– CIWIN as a secure voluntary/opt-in multi-level communication/alert system composed of two distinct functions: a rapid alert system and an electronic forum for the exchange of CIP ideas and best practices – clearly shows the most advantageous ratio between benefits and drawbacks. Obviously, such solution cannot work on its own. Firstly, its success depends on Member States willingness to act in the spirit of solidarity and share relevant information with those Member States who might need it. Secondly, it must go hand in hand with other parallel activities within EPCIP, such as for example regular meetings of expert groups (where the private sector, i.e. owners and operators of critical infrastructures, should be fully involved) and the development of criteria for the identification of critical infrastructures.

The CIP information sharing process among relevant stakeholders requires a relationship of trust, in such a way that proprietary or sensitive information that has been shared voluntarily is 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 is 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 cross border security oriented "state of mind".

It has to be stressed that CIWIN does not bring revolutionary changes into increasing EU security, and needs to be regarded only as one of many steps of the implementation of EPCIP. CIWIN is an IT tool designed to facilitate communication around CIP topics and provides functionalities such as news bulletin boards, discussion groups, collaborative environments, document and workflow management features that are part of everyday's internet or corporate intranet experience. The elaboration of CIWIN will consider a large number of features, while ensuring that their existence and use can be suppressed in situations where they are not seen to add value or they conflict with established practices. Fortunately, modern general purpose internet/intranet content management applications provide a wealth of possibilities to setup such a system, while keeping a range of options available to customise features according to country preferences and new insights on the best way of using the system. As mentioned earlier, CIWIN will be setup in the S-TESTA network[16], thereby requiring physical access to S-TESTA terminals

[16] A working level agreement already exists with DG ENTR to give CIWIN access on TESTA. This agreement will be formalized between DG JLS and DG ENTR upon approval of the CIWIN impact assessment.

located in government premises. CIWIN users will also require an account on the system. The user authentication will have to be performed according to the RESTRAINT UE security level.[17]

As regards the uptake of CIWIN by the Member States, it needs to be stressed that the CIWIN prototype, its look and functionalities, have been discussed regularly within the CIP Contact Points meetings. The discussions helped shape CIWIN into its current prototype version, tailored to different Member States' wishes and needs. The discussions helped to find a compromise solution between initially different opinions between Member States.[18] Throughout the discussions the prototype gained a lot of support among Member States, and it is expected that a large majority of them will be participating in the tryout of the prototype system, scheduled to start in the last third of 2008. The development of the prototype into a fully functional system is expected in mid 2009, after the conclusion of the testing period. .

For the success of CIP policies in Europe, it is evident that an EU approach, in addition to national approaches, is needed. The interconnectedness of critical infrastructures in Europe, hastened through the drive towards a single market, has brought unprecedented efficiency across the continent. That same interconnectedness, however, increases the potential for cross-border crises when infrastructures fail. It is therefore worth mentioning that the expected benefits from a regular exchange of information, best practices and alerts in this emerging policy will by far outweigh the envisaged costs. As mentioned before, CIWIN should prevent the duplication of CIP activities in Member States and allow Member States who are currently developing their national critical infrastructure policies to benefit from the experiences of other Member States. Without a European approach and co-operation among Member States, national CIP policies would develop separately and independently from each other, missing the opportunity to jointly develop definitions, practices and activities that could serve as a uniform model throughout Europe (in theory, without co-operation and the exchange of information, 27 vulnerability assessment methodologies could be developed throughout the EU in parallel, resulting in significant costs for national budgets).

As mentioned several times, the CIWIN initiative can not be separated in terms of content as well as in terms of costs and benefits from the EPCIP. With a better co-operation on CIP issues between EU Member States as well as CIP sectors (which is one of the objectives, CIWIN wants to achieve), some of the past critical infrastructure failures could certainly be prevented. [19]

---

17 A more detailed presentation of the CIWIN prototype's concept can be found in Annex IV.

18 For more on different opinions between Member states, see the results of the green paper consultation in Annex II and the excerpts from the CIWIN study in Annex III.

19 As an example, the effects Italian blackout in 2003 could certainly be limited to a much narrower scope with proper exchange of information. The 2003 Italy blackout was a serious power outage that affected all of Italy—except the island of Sardinia—for 9 hours and part of Switzerland near Geneva for 3 hours on 28 September 2003. It was the largest blackout in the series of blackouts in 2003, affecting a total of 56 million people. It was also the most serious blackout in Italy in 20 years. The Swiss Federal Office of Electricity admitted that the Italian power outage was triggered by the failure of a power line at the Lukmanier pass in central Switzerland. But it said this had been the result of an underlying lack of regulation in the European electricity market, with electricity suppliers failing to take into account the technical limitations of the power grid. There were reports of up to 5 deaths due to the lack of lighting and cost an estimated 120 million EUR. (source: JRC: "On Cross-cutting criteria for European Critical Infrastructures, 2008).

7.1. Respect for fundamental rights

The CIWIN as a secure voluntary/opt-in multi-level communication/alert system will be a secure classified system, able to contain information up to the level of RESTREINT UE. CIWIN will use the S-TESTA network for communications to Member States, thereby requiring end users to have access to S-TESTA connected terminals in government premises. Each CIWIN user will also require an individual account on the system and in order to build mutual trust they will require security clearance to at least CONFIDENTIEL UE.

The implementation of the preferred option means that data collected in the CIWIN system will be mainly of a non personalised basis (methodologies, best practices, risk assessment tools, CIP guidelines, imminent risks and threats etc) and will not give rise to any individual rights or obligations for individuals. The only collection and exchange of personal data concerns relevant CIP experts in Europe (e.g. those participating in the work of CIP expert groups) and is done on a voluntary basis. Their personal data would include the name and address of the employer and business address but nothing else. Therefore the respect for fundamental rights is not affected by the creation of CIWIN nor does the CIWIN implementation have any negative effects on the respect for fundamental rights.

Moreover, the data collected will be protected in accordance with data protection rules and shared only on a need to know basis where deemed relevant and appropriate, with EU Member States. (EU Member States authorities representing a specific industry sector will only have access to the list of experts within the same sector).

7.2. Costs of preferred option

As already mentioned, CIWIN will not have a relevant direct financial costs on either member States' or EU's budget.

Table 1: Costs for Member States' budgets

Direct costs for Members States' budgets		
Hardware purchase		
	Cost (in EUR)	Quantity
1 central computer	10,000.00	1
Personnel		
	Number	
CIWIN Executive	1 per Member State (part time)	
CIWIN Support Officer	1 per Member State (part time)	

Table 2: Costs for the EU budget

Direct costs for EU budget		
Maintenance costs of the system		
	Cost (in EUR)	
Hosting of RAS functionality of CIWIN system (secure environment)	Appx. 300.000 per year[20]	
Support and maintenance	250,000	2009 onwards
Personnel		
	Number	
CIWIN Administrator	0.5 AD	
CIWIN Technical Support	0.5 AST	
Contracted Studies		
	Cost (in EUR)	Year
Developing CIWIN prototype	250,000	2006
Developing a functional CIWIN system	500,000	2008
CIWIN – necessary technical support to security accreditation, maintenance, the provision of a helpdesk and training	400,000	2009

[20] The envisaged cost is based on an average calculation of the hosting, support and maintenance of some existing RAS, e.g. ERWS, RAS-BICHAT, RAS CHEM and CECIS.

8. MONITORING AND EVALUATION

8.1. Core indicators of progress

The following indicators of progress would have to be used in order to assess progress being made by CIWIN:

- Number of Member States participating in the CIWIN system (at least 20 Member States should use it regularly in order for the system to be deemed successful);
- The level of confidentiality of the information exchanged (are member States uploading only non-classified information or is classified information uploaded as well);
- Are CIP experts group using CIWIN as a main tool for the exchange of opinions in order to achieve their objectives (e.g. definition of the criteria to identify critical infrastructure in specific sectors)?

CIWIN shall be assessed against these indicators after the first 3 years of its establishment.

8.2. Possible monitoring and evaluation arrangements

The main monitoring and evaluation arrangement should focus on the "customer satisfaction" principle.

- After the conclusion of the testing period (CIWIN pilot project) in 2009, the Commission should send short questionnaires to Member States authorities in order to assess their satisfaction with the system and to verify whether it contributes to the general objectives of the CIWIN initiative(and proposals for possible new functionalities or deletion of the not well functioning).
- The functional system should then be reviewed by the Commission every 3 years. The Commission shall base its review on Member States' opinions obtained at the regular Critical infrastructure protection.

ANNEX I

GREEN PAPER

on a European Programme for Critical Infrastructure Protection

1. BACKGROUND

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

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

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

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

2. OBJECTIVE OF THE GREEN PAPER

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

The Green Paper provides options on how the Commission may respond to the Council's request to establish EPCIP and CIWIN and constitutes the second phase of a consultation process concerning the establishment of a European Programme for Critical Infrastructure

Protection. The Commission expect that by presenting this green paper, it will receive concrete feedback concerning the policy options outlined in this document. Depending on the outcome of the consultation process, an EPCIP policy package could be put forward during 2006.

3. PURPOSE AND SCOPE of EPCIP

3.1. The overall goal of EPCIP

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

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

Question

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

3.2. What should EPCIP protect against

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

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

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

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

Question

Which approach should EPCIP take? Why?

4. SUGGESTED KEY PRINCIPLES

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

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

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

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

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

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

Question

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

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

5. A COMMON EPCIP FRAMEWORK

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

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

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

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

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

- common CIP principles;
- commonly agreed codes/standards
- common definitions on the basis of which sector specific definitions can be agreed;
- common list of CI sectors;
- CIP priority areas;

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

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

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

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

Questions

Would a common framework be effective in strengthening CIP?

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

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

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

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

6. EU CRITICAL INFRASTRUCTURES (ECI)

6.1. Definition of EU critical infrastructure

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

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

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

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

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

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

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

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

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

Question

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

6.2. Interdependencies

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

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

Question

How can interdependencies be taken into account?

Do you know of any suitable methodologies for analysing interdependencies?

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

6.3. Implementing steps for ECI

The Commission would suggest the following implementing steps for ECI:

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

(2) Progressive identification and verification on a sector-by-sector basis of ECI by MS and Commission. The decision on designating particular CI as ECI will be taken at the European level[21] due to the cross border nature of the infrastructure concerned.;

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

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

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

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

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

Questions

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

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

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

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

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

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

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

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

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

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

7. NATIONAL CRITICAL INFRASTRUCTURES (NCI)

7.1. The NCI role in EPCIP

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

a) NCI is fully integrated within EPCIP

b) NCI is outside the scope of EPCIP

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

Question

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

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

7.2. National CIP programmes

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

Question

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

7.3. Single overseeing body

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

(a) A single CIP overseeing body;

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

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

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

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

Specific competences could include:

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

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

   i. the Commission

   ii. other MS

   iii. CIP owners and operators

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

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

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

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

g) Identify interdependencies between specific CI sectors;

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

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

Questions

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

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

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

7.4. Implementing steps for NCI

The Commission would suggest the following implementing steps for NCI:

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

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

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

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

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

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

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

Question

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

8. Role of CI owners, operators and Users

8.1. Responsibilities of CI owners, operators and users

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

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

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

(17) **Establishment, implementation and updating of an Operator Security Plan (OSP).**

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

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

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

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

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

The OSP could contain security measures arranged around two headings:

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

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

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

Questions

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

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

Are the suggested obligations proportional to the costs involved?

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

8.2. Dialogue with CI owners, operators and users

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

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

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

Question

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

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

9. EPCIP Supporting measures

9.1. The critical infrastructure warning information network (CIWIN)

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

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

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

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

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

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

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

used by the relevant MS CIP bodies and the owners and operators as a two way communication system.

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

Questions

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

Should CI owners and operators be connected to CIWIN?

9.2. Common methodologies

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

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

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

Questions

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

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

9.3. Funding

Following an initiative of the European Parliament (creation of a new budget line – pilot project « Fight against terrorism" – in the 2005 budget), the Commission took the decision on 15th September to allocate 7 Mio€ to finance a set of actions which will enhance European prevention, preparedness and response to terrorist attacks, including consequence management, critical infrastructure protection, terrorist financing, explosives and violent radicalisation. More than two thirds of this budget is consecrated to the preparation of the future European Programme for Critical Infrastructure protection, to the integration and development of capabilities required for the management of Crises of trans-national significance resulting from possible terrorist attacks and to emergency measures which may be required to address a significant threat or occurrence of such an attack. It is expected that this funding will continue in 2006.

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

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

The Commission is funding research projects in support of critical infrastructure protection in the Preparatory Action for Security Research[22] (2004-2006), and has planned more substantial activities in the area of security research in its proposal for a Decision of the Council and the European Parliament concerning the 7th EC Research Framework Programme (COM(2005)119 final)[23] and its proposal for a Council Decision concerning the Specific programme "Cooperation" implementing the Seventh Framework Programme (COM(2005)440 final). Targeted research which aims to provide practical strategies or tools for risk mitigation is of prime importance to securing EC's critical infrastructure in the medium to long-term. All Security Research, including in this area, will be submitted to ethical review to ensure compatibility with the Charter of Fundamental Rights. The demand for research will only increase as the number of infrastructure dependencies increase.

Questions

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

9.4. Evaluation and monitoring

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

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

---

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

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

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

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

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

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

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

Question

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

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

ANNEX II

Results of the EPCIP Green Paper – Member State comments

Twenty-two Member States provided official responses to the EPCIP Green Paper consultation process by the end of February 2006.

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

In general, most Member States felt that EPCIP's broad goal should be to raise CIP capability in Europe. EPCIP should support and facilitate work on CIP and should, in particular, provide the tools necessary to improve the protection of critical infrastructures.

Below is the analysis of the green paper, relevant for the present work on CIWIN.

Key principles (question 4)

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

Nineteen Member States generally supported the five key principles identified in the EPCIP Green Paper although nine of these Member States proposed to make slight revisions to the text. Several Member States underlined the importance of the confidentiality principle especially vis-à-vis the private sector. Three Member States did not offer any specific comments on the list of principles.

A number of Member States identified additional key principles, which could also form the basis of EPCIP. These could include:

- Sector-by-sector approach - To assure complementarity to existing measures and respect for the differences between the CI sectors, the development of EPCIP and initiatives under EPCIP should to the largest extent possible be anchored in the relevant CI sectors.

- Effectivity;

- Coordination – the European Commission will play a coordinating role in EPCIP.

To what extent should such a common framework be obligatory and to what extent voluntary?

The Member States were divided concerning the issue of whether EPCIP should be of a voluntary or obligatory nature. Seven Member States (were of the opinion that parts of the common framework could be obligatory. Views varied however concerning exactly which parts of the framework could be obligatory (some Member States underlined that those parts referring to ECI, others that those parts having a strategic importance). A further two Member States were of the opinion that the framework could be voluntary at first and become

obligatory once it is tested and well established. Five Member States supported a voluntary approach for the common framework. Eight Member States did not present clear views on this issue.

Implementing steps for ECI (question 6.3)

The Member States were divided concerning the usefulness of the implementing steps proposed in the Green Paper. Thirteen Member States found the proposed steps acceptable although a number of modifications were proposed. Three Member States were of the opinion that it is currently too early to develop such steps when the principles and definitions have not yet been agreed. Three Member States disagreed with the proposed steps. Three Member States did not present a clear opinion on this subject.

Two Member States highlighted in their responses the need for a risk analysis process.

The role of the Commission was generally seen as that of a facilitator. In the eyes of the Member States, the Commission should actively contribute to the ECI designation process. Among the tools which could be used by the Commission is facilitating the exchange of best practices, providing experts, funding the necessary research work and participating in relevant meetings. The Commission could be seen, according to one response, as a driving force of the process.

In reference to the question on the legal status of the designation of ECI, six Member States were of the opinion that a legal decision is needed in order to designate ECI, three were against and the rest did not provide a clear view.

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

The Member States did not have a uniform view concerning the setting up of the CIWIN network. Out of the responses received:

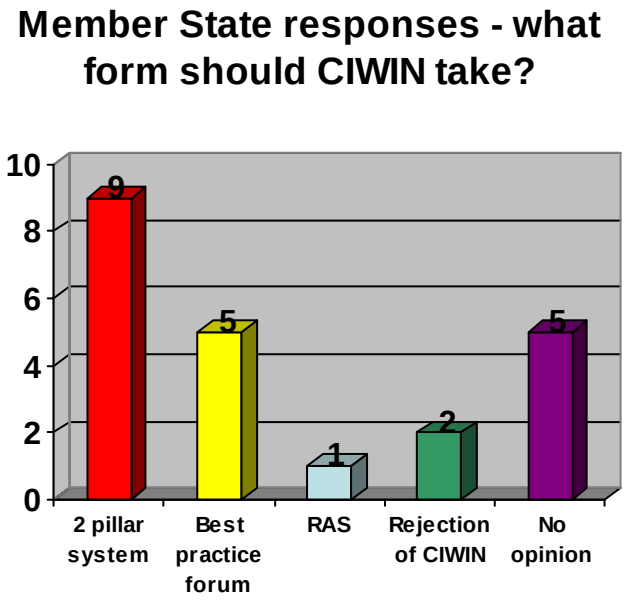
- Nine Member States supported the setting up of CIWIN as a multi-level communication/alert system composed of two distinct functions: a rapid alert system and an electronic forum for the exchange of CIP ideas and best practices. A number of Member States underlined however the need to take a step-by-step approach to the process of setting up the network.

- Five Member States favoured limiting CIWIN to a forum for the exchange of CIP ideas and best practices;

- One Member State felt that CIWIN should be set up as a rapid alert system (RAS) linking MS with the Commission;

- Two Member States completely rejected the idea of setting up CIWIN in any shape;

- Five Member States did not offer a clear opinion on this issue.



In reference to the issue of connecting CI owners/operators to CIWIN, fourteen Member States favoured linking CI owners/operators to CIWIN. Out these responses, two Member States underlined their support for connecting CI owners/operators to CIWIN only if CIWIN was limited to a forum for the exchange of best practices. Moreover, a number of Member States underlined that different access levels should be given to different types of organizations connected to the network. Five Member States did not see a need to connect CI owners/operators to CIWIN. Three Member States did not offer comments concerning this issue.

ANNEX III

Relevant excerpts from the CIWIN study

1. Main findings concerning CIWIN as a platform for the exchange of CIP information

This part of the report is built on the answers to the interview questions provided by the visited Member States. For every question, there is a quantitative and qualitative analysis of the collected feedback. The review of this feedback has ultimately an impact on the implementation of the CIWIN system and/or its terms of use. The implications for the CIWIN are therefore documented as a list of requirements derived from the MS statements. These requirements will be covered by operating procedures and supporting documentation rather than being enforced by the CIWIN system business/security logic.

1.1. Different views on whether the system should be an open platform, a secure platform or a combination of both.

The Member States have divergent views on whether or not the CIWIN system should be an open platform for the (unsecured) exchange of CIP related information or rather ha closed platform for the secure exchange of CIP related information between a limited number of users, or a combination of both.

CIWIN as an open platform

Three countries are in favour of this view on CIWIN. The main reasons expressed by these countries are:

- *Different channels will be used for classified information:* if information is classified, it will be exchanged through other channels (diplomatic etc), not through a European-wide system.
- *No need to classify best practices on CIP:* the vast majority of this information does not require any particular measures to limit its distribution as this is publicly available information or information –if made public- that is harmless.
- *Need to have access to a wide community:* if only a limited group of users has access to the system, the quantity and quality of the information will be problematic. There is a need for a wide cross-European CIP community, with contributors of both the private and the public sector.
- *Some existing platforms on CIP are open platforms:* reference is made to US web portals where CIP related information is freely made available to any type of user.

All these countries are as such not opposed to the system as a combination of an open platform and a secure system, but have said that they will not use the secure system for the exchange of best practices. One of these countries mentioned it might revise its position if the business need for a secure system is clearly demonstrated. Another one of these countries sees

the combination of an open platform next to a secure system as a possible compromise with other countries who would want a secure system.

CIWIN as secure system with a limited user group

Nine countries are in favour of this view on CIWIN. The main reasons of the view expressed by these countries are:

- *(Some) CIP related information is classified:* this information cannot be put on a public website.

- *To exchange (some) information, the receiver of CIP related information must be known:* This argument also counts for non-classified information. The reasons most often mentioned are the need for *trust* before CIP related information is exchanged and the existing *national rules and obligations* on the exchange of sensitive information.

- *Other channels already exist for those who want to make some information available to a wider (CIP) community:* Member States can make information available to users in their countries if they want to through the internet, a national CIP network etc.

- Some existing national CIP systems have restricted access as well.

- *The added value of an open forum is not understood:* the tangible advantage of such a forum is unclear to some Member States.

CIWIN as a combination of an open platform and a secure system with a limited user group

For security reasons it is not possible to build one system that is both public and secure. This option should thus be understood as the creation of a public web portal next to a secure system, without any interface between those two. Twelve countries are in favour of this view of CIWIN. The main reasons mentioned are:

- *Different levels of access to information are needed:* depending on the type of role a person has, a person may have different information needs. Depending on the information, access should be given to the wider public, to a more limited group or to a very restricted group.

- *Awareness raising:* making information available to the wider public helps awareness raising concerning CIP in Europe.

However, there is some divergence within this group of countries on certain matters related to this solution:

- *Priority of public versus secure part:* There are different views on which part of the system is of primordial importance: some find the public forum most important and the secure platform an added value, whereas others would rank them in the opposite way. Next to these groups, a considerable number of countries did not formulate a clear preference for either part of the system.

- *Public platform as interactive or one-way information channel:* Some countries see the public platform disposing of the same functionalities as the secure platform: discussion threads, message boards, contact information etc. The main criterion for not making information available on the public forum would for these countries be the security classification of the document or the sensitivity of its content. Other countries rather see this as a web-site with general CIP information for the wider public.

1.2. Implications for the CIWIN system

Taking into consideration the divergent views of the Member States and the initial definition of the CIWIN system, the primary idea of having an open system has been abandoned in favour of CIWIN being a secure system. As some Member States indicated in their answers the value of public non secure access to CIP information, the requirements will not be addressed directly by CIWIN but instead by a separate public site constructed separately from CIWIN. This public site will operate independently of CIWIN without any connections with the secure system to avoid compromising the integrity of CIWIN's security setup.

***Requirement** 1: In case of conflicting CIP information access requirements, the CIWIN system will give priority to features and functions that enforce the protection of the information confidentiality and support the development of trust between members of the CIWIN community*.

CIWIN must allow different MS to apply different approaches to the distribution of information. Member States should have the option to share information according to the terms set by the owners of the information.

***Requirement** 2: The owner of information placed in CIWIN determines who has access to it.*

This requirement captures a fundamental principle governing the access control rules for all information items held in CIWIN. This is tightly related to the "need-to-know" principle introduced in the definition of the CIWIN system. (this aspect is reviewed in more details further down in the document)

This approach allows owners of CIP information to determine the scope of members that have access to the information made available in CIWIN. The scope can be set to from everyone (public within the CIWIN members) down to specific individuals for highly sensitive information.

1.3. Different views on the security measures needed for the CIWIN system

Description

There are diverging views between the Member States on what should be the highest security classification of documents exchanged through the system. First of all three countries that are in favour of an open platform do not see a need for the system to foresee measures to exchange classified information. However, two of these three countries did identify a highest classification level they deemed most appropriate in case there would be a secure system built. For this reason, their answers are included in the results for a secure system as well.

Eighteen countries have identified the level of EU restricted as the highest level of security classification required for documents exchanged through CIWIN. Some of these Member States indicated that they prefer the system not to contain documents of a higher security classification as this implies strict security measures that would limit significantly the access to the system and its ease of use.

Four countries however identified EU confidential as the highest level for security classification of documents exchanged through the system. The reasons mentioned by these Member States is the concern that certain types of information may have to be classified at an EU confidential level, for example certain lessons learnt or more detailed information.

Finally, two countries have identified even higher security levels needed for documents to be exchanged through the system; one requested the level of EU secret, whereas another one requested the level of EU top secret.

Although a considerable group of Member States would find the level of EU restricted satisfactory for the system, it is apparent that there are some very divergent views on the likeliness of the classification of the information that will be exchanged through the system. This divergence of views may follow from differences in expectations regarding the information to be exchanged, from different traditions in dealing with CIP information, from the all-hazards approach of EPCIP which includes terrorism and from different interpretations on what measures follow from security classifications of documents:

- *Different expectations on type of information exchanged:* As will be further explained in the section dealing with the type of information to be exchanged, there are some divergent expectations between the Member States on what type of information will actually be exchanged through the system. Especially the level of detail of the information exchanged will determine to a large extent what security classification should be appropriate. The fact that two countries indicated very high security levels for the system, may indicate that they also expect concrete information on ECI vulnerabilities will be exchanged through the system.

- *Different traditions in dealing with CIP information:* Whereas in some countries there is a tradition of openness towards the public concerning the protection of CIP, other countries prefer not to share any information on the topic with those who are not directly involved in CIP. This difference in appreciation has as a consequence that the same document might be classified in one Member State, whereas it is considered open for consultation in another Member State.

- *All-hazards approach, including terrorism:* The general approach of the EPCIP programme is to protect ECI against all types of disruption or destruction[6], ranging from a natural event to a human-caused accident to a terrorist attack. The fact that the CIWIN system would allow for the exchange of information regarding the protection of infrastructures against terrorist attacks has as a consequence that the distribution of such information to unauthorised users entails a higher security risk than when it concerns the protection against a natural event. In some Member States the current focus of CIP may be more on the protection against natural events and human accidents, whereas in other countries the focus of CIP may lay more on the prevention and protection against terrorist threats. - *Different interpretations of security levels:* Although the security levels mentioned in the Interview Guide of the missions have been clearly defined at the European level, it should not be excluded that the people met in the Member States may

have different interpretations of what security measures follow out of each classification level. This was illustrated in several countries where the level of EU restricted was indicated as sufficient but where it was also mentioned that the users dealing with this information should have a security clearance. On the other hand, Member States indicating the level of EU secret and EU top secret could possibly be not fully aware of the consequences this has on the accessibility and the number of users of the system.

It should also be noted that some countries mentioned legal constraints for their public servants to exchange classified information. These constraints may deal with sharing such information with others in the first place, but also with the subsequent use and distribution of such information. For example, a country mentioned the legal obligation for its civil servants to share any information received that is not considered as pivotal for the national defence with the press – simply upon request of the latter.

Implications for the CIWIN system

Indeed the concern of some Member States vis-à-vis the security of the system is justified by the fact that some of the information to be exchanged through CIWIN could be of a very sensitive or confidential nature. In order to reinforce security of the communication between CIP MS official actors and experts, CIWIN must allow CIP information to be classified and enforce the rules applicable to the level of classification.

***Requirement** 3: CIWIN must be capable of supporting multiple levels of classified information. The initial level is EU restricted and more levels may be added in the future. The CIWIN Architecture must allow for extensions to higher levels of information access control. Higher levels of access control must be achieved by extending the system, without the need for redesign or reimplementation.*

CIWIN will be setup in the S-TESTA network, thereby requiring physical access to The CIWIN Concept Document

1.4. Different views on the accessibility of CIWIN

Description

In general terms, the composition of actors potentially involved in CIP (the country's "CIP community") in the different EU Member States turns out to be rather similar in the Member States. Next to a coordinating body, the responsibility for the protection of critical infrastructures lies with the different ministries/departments/agencies responsible for the sectors. These authorities may be regulatory authorities and supervisory authorities. Depending on the state structure of the country, these ministries/departments/agencies are located at the national level or at a sub-national level. Also depending on the country, the coordinating body has a strong role in the country's CIP policy or rather facilitates any cross-sector CIP discussions with participation of the different ministries/departments/agencies. Next to these governmental actors, countries try to involve the private owners and operators of the infrastructures but do so in very different ways. Whereas in some countries the private sector actors are very closely involved in policy making regarding to CIP, in other countries their role is limited to the execution of the policies designed by public sector actors only.

The Member States have however very different views on the accessibility of CIWIN in terms of limiting access to the system or not, in terms of which type of users should be given access and in terms of the rights attributed to a user when given access. Next to that, there is a

general request for clarity in the direct and indirect access management of the system. One country did not provide the study team with an answer on this question, stating that it will determine in each different case which key persons are to have access to the system.

Limited access or not?

This discussion is directly linked with the discussion on whether or not the CIWIN system should be an open platform or not. Therefore, it is the same countries which are in favour of an open platform who do not want to limit the access to the system.

Types of users to be given access

- European Commission and CIP contact points

The Member States have diverging views on the degree of penetration of access rights to the system in the countries. With the exception of one country, there is general agreement amongst the Member States on granting access rights to authorised users at DG Justice, Freedom and Security of the European Commission. However, the Member States do ask that the role of the Commission regarding the system will be clarified (e.g. will the Commission hold administrator rights or not, etc.).

There is unanimous agreement between the Member States that the country's CIP contact points will be granted access to the system.

- Ministries/departments/agencies in the Member States

With the exception of two countries, there is general agreement that users may as a principle also be located in the ministries/ departments/agencies responsible for the sectors. The main reason for the opposition of the two countries is that they want to keep control on the information flow through the system –as is described in further detail in the part discussing the different views on the access management of the system. When identifying this type of users, the Member States did however express different views on how to translate this in concrete terms:

In some countries the potential users of the system are seen as officials working on the protection of critical infrastructures with cross-border interdependencies, whereas in other countries the users are seen as officials working on the protection of any type of critical infrastructure as well. This clearly has an impact on the potential number of users in each country.

In some countries the ministries/departments/agencies have a crisis management unit available, responsible for the coordination of crises in the sectors for which it is responsible. Although the officials working on the protection of critical infrastructures may not necessarily be working in this crisis management unit, some countries have expressed the view that the access point of the system should be in this crisis management unit. It is possible that there was some confusion between the forum and rapid alert functionalities when this answer was given.

In some countries with a federal state structure the users are seen as officials working in the ministries/departments/agencies at the national level, whereas in other countries the users are also seen at ministries/departments/agencies at the sub-national level.

- EU level expert groups

There is less agreement between the Member States on granting access to EU level expert groups. Twelve countries were in favour of this option. Three of these countries indicated a medium to low priority for their choice. The countries in favour of this option made some additional comments:

When access is given to these experts, it should be foreseen that they have only access to the information they need to perform their tasks, and not to all information available on the system.

There is a practical problem with granting direct access to the system to those experts who are not officials. If the system is made available on a platform like S-TESTA, private actors will not have direct access as this system is available to public services only.

One country indicated that the experts given access to the system should not belong to the private sector.

The main reasons mentioned by those countries not in favour of access by EU experts were:

- Other channels exist for the exchange of information between the EU experts.
- Private actors should not be given access to the system as this risks abuse or diverting of information for commercial use.
- The more users are given access to the system, the higher the risk of security breaches.

- Owners/operators of critical infrastructures

A relatively small group of around seven countries are in favour of granting owners and operators access to the system. Some of the Member States in favour of this option indicated a low priority for their choice or suggested to grant these actors access in a second or third phase of the implementation of the system.

The country's positions on granting owners and operators access to the system does not change when asked about granting access to state enterprises and other semi-governmental agencies in charge of critical infrastructures. They are thus considered to be treated on an equal basis with private owners and operators.

The reason mentioned by most countries against granting access to these users is that it is the Member State's responsibility to inform the owners and operators of critical infrastructures of any relevant information that may enhance the protection of the infrastructure. In case of a critical infrastructure located at the European level (e.g. Galileo), the European Commission is expected to fulfil this role.

Direct and indirect access management of the system.

- Direct access management

There is a general request from the Member States to foresee a clear solution for the management of access rights for the CIWIN system. Most of the Member States request a

national approval for users of the system within their country. There are several reasons behind this request:

- Member States consider themselves as best positioned to judge who would be a relevant user for cross-European exchange of CIP related information within their country. They are also best informed about possible changes of people or responsibilities, making a quick update of access rights possible.

- In order to limit the security risks of unauthorised people becoming users and accessing classified and/or sensitive information, Member States expect a formal approval of every user, guaranteeing that this person will not misuse or further distribute the information.

- Some Member States see it as a way to control the flow of CIP related information going out of the country. Some Member States fear that -even if the system is designed for the exchange of classified information- there remains a risk for human error in making classified information available to unauthorised users. By controlling the number and type of users of the system, these Member States feel that the risk that one of their nationals will make a human mistake is more easily mitigated.

Next to the request for national management of access rights, the need for a user-friendly, time efficient and rapid registration management for applicant users is also apparent.

It is clear that -next to the practical advantage of being best informed of the composition of their national CIP community- attributing direct access management to the Member States helps to build trust and gain confidence in the system and its users. The risk that this entails is that Member States will use different criteria for granting access to national users. Even with the establishment of common procedures the different views that Member States have on the system's users (see part on 'types of users to be given access') will mean that in some countries a wide community will be given access to the system, whereas in other countries a very restricted group will be given access.

Finally, it should be noted that the Member States have different visions on the rights a (type of) user should have once granted access to the system. This issue will be addressed in the part discussing the views on the administrator and user rights.

- Indirect access management

All countries mentioned that they intend to share some of the information made available through the CIWIN system with the members of their national CIP community (e.g. owners/operators) on a "need to know basis". This sharing of information could be in an aggregated way or not, depending on the type of information, its security classification and the type of national recipient of the information. This means that information available in the system will be distributed – in one way or another- to other actors, who therefore become indirect users of the system.

The existence of indirect users of the information made available through the CIWIN system may impact the trust of some countries in sharing classified information through the system. Although a sender may know the direct receiver of the information, he/she will not know whether or not this end user will share this information with indirect users, whether the information will be aggregated or not, how this information will be transferred (electronically, on paper,…), etc.

Another consequence of indirect users of the system is that the management of information flows between the CIWIN system and these indirect users may become heavy, especially in those countries who allow only a restricted number of users to access the system. It is questionable to what degree the indirect users of the system will be able to contribute their knowledge to other (direct and indirect) users if the number of direct users is highly restricted in a country.

Implications for the CIWIN system

In order to address all the concerns brought up during the mission to the Member States, the CIWIN system will support different types of users allowing to separate key business actors involved in the use and administration of CIWIN. The first type of user is the CIWIN Executive.

Requirement 12*: CIWIN will support the user type* CIWIN Executive*. This type of user forms the basis for the business administration of CIWIN. The CIWIN Executives have the rights within their Member State to add new members to CIWIN and delegate their administrative rights. The CIWIN Executives intervene in the workflows related to the exchange of information between Member States and thereby can act as gatekeepers for information flowing (in and) out of the country. The CIWIN Executives will also manage the contact list for their country*.

The CIWIN Executive will be the responsible person representing a country within the CIWIN community. The CIWIN system membership is initially formed by the set of 28 CIWIN Executives, one for each Member State plus one representing the Commission. The Executive has the choice to remain the only representative within CIWIN of his national CIP community, or to extend CIWIN membership by adding the national CIP actors.

It is anticipated that the role of CIWIN Executives will evolve over time as best practices for the use of CIWIN become more apparent. Initially, the Executive will form the original set of members and determine how the national CIP communities interacts with CIWIN and how the basic administration rights are delegated to the appropriate national authorities.

The CIWIN system limited to the CIWIN Executives corresponds to an extreme approach providing a little more than a new redundant formal system for international communications. As the purpose of CIWIN is to enable communication within the CIP community, CIWIN will support additional types of users which will have specific rights.

The first direction of CIWIN membership extension is towards governmental officials dealing with CIP matters. Theses extensions would be based on national sectoral responsibilities and, in some cases, sub-national CIP responsibilities.

Requirement 13*: CIWIN will support the user type* ***CIP Official*** *(official in the sense: person appointed or elected to an office or charged with certain duties). This type of user will be members consisting of government or supervisory authorities' officials involved in CIP. These memberships are not limited in time or restricted to specific activities. The Officials will have their scope of accessible information limited to the sector they are assigned to.*

The officials will have access to all the functions of the CIWIN system with restrictions on the accessible information based on their sector. Next to the officials, the CIP community will include CIP experts provided with a temporary membership for the purpose of participating in a specific CIP activity such as a CIP Expert Working Group or a CIP project.

Requirement 14*: CIWIN will support the user type* ***CIP Expert****. This type of user is characterised by a time limited membership and access restricted to information relevant to their assignment.*

Requirement 15: *CIWIN will maintain a list of members. Initially, the list is only visible to the CIWIN Executives.*

1.5. Different views on the type of information to exchange through CIWIN

Description

The Interview Guide contained several questions with the purpose to identify the type of information the Member States wish to exchange through the system. The questions dealt with information related to best practices related to CIP and other types of information.

Best practices related to CIP

A best practice is a concept based on the principle that to reach a certain result there exist techniques, methods, processes, activities or initiatives that have proved from practical experience to be more effective than other ways to reach the result. The idea is that –when applying best practices- one can realise an objective with less problems and unforeseen obstacles than when applying other methods. Best practices are sometimes put in a pre-defined template and may be characterised by a certain form of quality label.

With the exception of one country, most countries are interested in seeing almost any type of best practices shared through the CIWIN system. Some countries have certain specific remarks on certain types of best practices. More importantly however, there are different views on the level of detail that these best practices should (be allowed to) contain - as already mentioned in the part discussing the security requirements for the system. Some countries specifically mentioned that they expect the best practices to remain on the general policy level, thus not containing any description of e.g. concrete protection actions. Other countries however expect more practical information, e.g. technical studies on the protection of infrastructures against explosions, concrete case studies on CIP implementation etc.

Although all types of best practices have been indicated as interesting by most Member States, the following best practices were most often mentioned and/or received the highest priority:

- Best practices that may help the Member State's implementation of actions related to the EPCIP. Only one country was not in favour of this option.

- Best practices related to the identification and designation of ECI in each Member State. Three countries were not in favour of this option.

- At the time of the execution of the missions to the Member States, the discussions concerning the proposal for Directive on the Identification and Designation of ECI were still going on. It is clear that the Member States see an important role for the CIWIN system in supporting the next steps foreseen by the EPCIP once the Directive is approved.

The other types of best practices have still received a considerable support by most Member States, be it sometimes with a somewhat lower priority. Below are the main comments made by the Member States for some types of best practices.

Best practices related to the identification and designation of critical infrastructures.

Some countries have mentioned that the criteria on the identification of critical infrastructures themselves are highly classified information and should not be put on the system. The reason behind this is that if the criteria are known, it will become easier for terrorists to identify these critical infrastructures.

Best practices that may help in the establishment of the National CIP Programmes

Although the number of countries against this option remains rather limited, this option turned out as the least popular type of best practices. Four countries are not in favour of this option. The main reasons for their opposition are:

- The establishment of national CIP programmes is a national competence, and the CIWIN system should not exchange information on this matter. This comment is related with the position that CIWIN should only deal with information on which the European Union has competencies.

- The system should not duplicate any information already available elsewhere. Information on the establishment of national CIP programmes is already available through the OECD.

Best practices that may help in conducting vulnerability, threat and risk assessments

This option turned out to be the second least popular best practice amongst the Member States, with three countries not in favour. The main reasons for their reservations are related to concerns of the security classification of this type of information.

Best practices related to interconnectivities of critical infrastructures

Most countries give a high to medium priority to this option. One country made the remark that this type of information should only deal with cross-border interconnectivities between critical infrastructures, not with interconnectivities within one country. This comment is related with the position that CIWIN should only deal with information that is at the European level, not the national level.

Other types of best practices requested by the Member States

Additional types of best practices requested by the Member States are: best practices on procedures/ways to implement policies and include stakeholders, different types of lessons learnt, information on crisis management, technical studies, risks related to CBRN etc.

Finally, several countries also indicated that the priority for certain types of best practices is likely to change over time. Whereas at the time of the missions to the Member States the most urgent type of best practice was related to the next steps envisaged after the approval of the Directive, other priorities may apply within a few years time.

Documents and other information

Two countries have the position that there is no need to make further background information on CIP related matters available on the system. The main reason for their position is that all this information is already available on the internet.

The other countries are open to sharing many different types of possible documents and other information through the system. The main findings are summarised below:

- *Avoid any duplication of information available.* A lot of the information mentioned is already available on the internet. Member States ask not to duplicate this information in the system, but to provide web links to this information.

- *Possible added values* identified of collecting this information in the system in comparison to searching for it on the internet is that there would be one place where this information is available (CIP one stop shop), and that this information will be EU-centred -in contrast to a lot of information on the internet which is US-oriented.

- There is a *high demand for making the findings of studies financed by the European Commission related to CIP available* on the system. It was mentioned that Member States are rarely informed of the results of studies that are launched by the European institutions.

- There is also a *high demand for making information on EU legislation/policy documents related to CIP* available on the system, preferably by providing web links to the relevant web sites.

- Information on *Member State's national legislation* and policy documents related to CIP, as well as on their *organisational set-up of the CIP community* is most important for those countries that are in the process of establishing or revising their national policy concerning CIP.

- The type of background information for which there is the *least demand are press releases, briefings and information packages prepared in the Member States*. Only fifteen countries are in favour of this option. It should however be noted that some countries indicated that the information packages of the Member States are of higher importance than the press releases.

Contact details

One of the questions asked to the Member States deals with making contact details available in the system. If a Member State is interested in doing so, it is asked to which level contact details should be allowed to be shown. This may thus include contact details of users and of non-users of the system.

Four countries are not in favour of making any contact details available through the system. The main reasons for their refusal are:

- *Control over information exchange:* if contact lists are made available through the system, users will tend to contact each other and start exchanging information directly. Some Member States want to control any outgoing CIP related information from their country and therefore do not want to make such contact details available.

- *Avoidance of any duplication with existing international contact lists:* Some international contact lists already exist for certain (sub-) sectors mentioned in EPCIP. It is feared that contact lists made available in CIWIN might be different from the existing contact lists e.g. Meridian contact list. In order to avoid any such duplication, some countries prefer not to make contact information available through the system.

- The other countries in favour of making contact information available through the system do however have different views on how this should be organised in concrete terms:

- *Making contact lists available on the open platform:* Although many countries would like to see a combination of an open platform and a closed system, very few countries (two) are interested in making contact information available on the open platform. These countries follow the principle that any user should choose whether or not to make his/her contact info available. Some other countries are explicitly against this principle.

- *CIP contact point/CIWIN Executive as gatekeeper:* Four Member States are keen on keeping control over any exchange of information between a user in their country and another user of the system by providing only the contact information of the CIP contact point. For those in favour of a certain degree of 'gate-keeping' by the CIP contact point, some see this as a very stringent role (meaning that the CIP contact point will serve as the sole contact point for the country) or as a way to keep an overview (meaning that the first contact should take place through the CIP contact point, whereas subsequent communications are allowed to take place directly with other users of the system). In the latter case, the CIP contact point would expect to be informed of all major subsequent communications.

- *Level of contact information made available:* The countries in favour of making contact information available of other users than just the CIP contact point of their country, hold different views on the level to which contact information should be made available. Four countries are in favour of showing the contact details of any user who so wishes. Others see it up to the level of representatives of the sectors. Three countries are interested in contact details of owners and operators of the critical infrastructures. *Individual contact details versus generic contacts:* Some countries specifically requested that no individual contact details would be made available, but only generic e-mail addresses and telephone numbers of the departments responsible for the sectors of critical infrastructure.

Implications for the CIWIN system

It is useful to restate that the scope of information contained in CIWIN is intended to be limited to best practices. Therefore, any information specific to CI and intelligence related to anti-terrorism measures and operations are not destined to be stored in any way in the CIWIN system. The information excluded from CIWIN includes the list of CI sites and their vulnerabilities.

Requirement 16*: The CIWIN system terms of use will exclude specific CIP information that can be considered as anti-terrorism related intelligence. It should not be possible to determine specific vulnerabilities and security characteristics of a specific CI site based on the information held in CIWIN*.

There are two aspects of the exchange of information: the type of exchanges that will be foreseen, and the CIP structure that CIWIN will place on the content of the exchanges.

The country feedback regarding the type of information exchanged through CIWIN is more relevant to the intended use of the system than to the system requirements themselves. However, the CIWIN system has an important role in structuring the way information is exchanged and stored in the system.

Next to the methods of exchanging information discussed further down, CIWIN will facilitate the exchange of information by structuring the content around the following areas:

Requirement 17*: CIWIN will provide an area dedicated to each **sector** including a news bulletin, a discussion group. CIWIN will also provide an area for matters addressing all sectors (cross-sector area).*

Requirement 18*: CIWIN will provide an area dedicated to **the library**. The library area will be the repository of CIP documents contributed by the members. The library will include a news bulletin board, a discussion forum, and procedures for accessing the documents. The library procedures will enable searching, viewing, creating, requesting access of/to documents. The library will also provide capability for discussion forums for each document for the collection of comments.*

Requirement 19: *CIWIN will provide an area dedicated to **external relations**. This area will include a news bulletin board and discussion forum on topics related to the exchange of CIP information with countries outside the EU.*

Requirement 20: *CIWIN will provide an area for **CIP Contacts**. This area will contain the list of contacts with its administration procedures. Access to this area will be subject, like other documents held in CIWIN, to access control rights. Initially, the contact list is only accessible to CIWIN Executives and restricted to their domain of authority (Member State or supervisory authority). The distribution and use of contact information within the CIWIN environment is determined by the CIWIN Executives.*

Requirement 21*: CIWIN will provide an area dedicated to the **CIWIN Executives**. The area will include a news bulletin board and a discussion groups for topics related to the best practices regarding the use of CIWIN. The CIWIN Executives area will also include the procedures for the administration of users (creation, extension, termination of CIWIN registrations) and areas (access right to each area).*

In addition to the areas listed above, CIWIN will provide support for areas created for specific purposes. CIWIN will support the following dynamic areas:

Requirement 22*: CIWIN will allow for **specific topic** areas. This type of area is intended to host restricted/private exchange of information on a specific topic. The creation of a specific topic area, combined with access rights to the area, ensures the exchange of information is contained within the area members. The areas will contain a news bulletin board and a discussion group.*

Requirement 23***:*** *CIWIN will allow for **CIP Expert Working Groups** areas. These areas are dedicated to specific working group activities and contain a news bulletin board, discussion group and procedures for supporting the administration of the working group.*

Requirement 24***:*** *CIWIN will allow for **EPCIP project areas**. These areas are dedicated to the implementation of EPCIP funded projects and they will include a news bulletin board, a discussion forum and procedures for communicating the project status.*

Requirement 25*: CIWIN will allow for **CIP** Alerts areas. These areas, initiated by the RAS system, will enable the contribution of the CIP community to the analysis and management of alerts. A CIP alert area will contain a news bulletin board and a discussion forum. The*

access to the area will be determined by the RAS based on the nature, importance and scope of the alert.

The CIWIN user will need to be guided into the CIWIN system based on his/her profile.

Requirement 26*: CIWIN will provide a personalised home page for each user. The personalised page will provide an overview of the users accessible areas, generic CIP news, access to email and process notifications (approval requests, access grant notification).*

1.6. Different views on the administrator and user rights of the system

Description

Forum administrator rights

As described above, the Member States generally expect to have a certain degree of control. This control does not limit itself to the control on the designation of the users in their country who will be given access to the system. Some countries also request stringent control on the information that these users will make available through the system, whereas other countries are more liberal on this matter. The Member States requesting strict control over any information made available through the system typically expect to have rights on editing, deleting and moving information put on the system by the users of their country. In fact, many of these rights requested by the Member States boil down to the fact that they request administrator rights towards all users of the system in their country.

A forum administrator typically has the ability to edit, delete, move or otherwise modify any thread or document posted on the forum. Administrators also usually have the ability to close the board, modify the board, and ban, delete, or create members of the platform.

When asked about the administrator rights, the Member States referred to several levels at which they feel that administrator rights should be granted, being:

- *The European level*: an administrator has to be identified for the general management of the system. There is no agreement between the Member States on whether or not this administrator should be allowed to delete any information put on the system. Eight countries are opposed to having an administrator of this level deleting information without consent of the owner of the information (country, department or person). The countries in favour of a European administrator of the system who may potentially delete information, do request however such an administrator to always inform the owner of the information of the deletion.

- *The national level*: although this is not a unanimous request by the Member States, the missions have unveiled that a considerable group of Member States feel strongly about having a national administrator who could control the information flow of users within the country to other users of the system (both within the country and abroad). The national administrator is seen to have all administrator rights mentioned above for all users within the country.

- *The level of the sector within the country*: For several reasons, some countries rather see the administrator rights held per sector within their country. The reasons for this are diverse:

- Practical reasons: As described above, some countries envisage a considerable community to be granted access to the system within their country. As the information flow of this community would be too large and too diverse to be controlled by a limited group of people, some countries prefer to delegate the national administrator rights to people responsible per sector.

- Different interpretation of administrator rights: Some countries interpret the rights of an administrator as equal to those of a forum moderator. In terms of the CIWIN system, forum moderators typically have a subset of the powers of a forum administrator, which may include editing, deleting, and moving threads, warning members for offences, and changing minor forum details. As it is often possible for moderator privileges to be delegated to other forum members, some countries see the different sector responsible to be best placed to fulfil this function.

User rights and role

Whereas some countries view the users as disposing of equal rights in the system, most countries prefer to foresee different levels of user rights. Based on a user's profile (role), the user has extensive or limited rights within the system. Reasons mentioned for different rights attributed to users are:

- *Need- to- know basis:* Although some countries do not see a need to limit access to certain types of information to any user of the system, a majority of the Member States has the opinion that information should only be available on a need-to-know basis. Based on the users' profile (role), a user should thus only be allowed to read the information he/she is entitled to see.

- *Expertise related to the topic:* Although some countries are wary about limiting contribution possibilities about a certain topic too much, most countries prefer to limit writing rights to those with a certain level of knowledge or activity concerning the topic.

- *Second-line control of outgoing information:* Although this is not a general request by all Member States, some Member States would like to foresee a two-step process before information (e.g. a document) is made available on the system. The reason for this varies: for some countries the reason is security (avoid that sensitive information is made available without formal approval) for others it is a way to enhance the quality of the document by allowing more knowledgeable users to contribute to the document as well.

- *Structuring of exchange of information:* for those areas of the system in which several actors have to work together in order to obtain a certain result or discuss on a topic, some users are expected to have certain rights allowing them to structure the collaboration and exchange of information (e.g. end the contributions to a document/stop a discussion etc.)

Implications for the CIWIN system

In order to satisfy the demand of most Member States, the CIWIN's users' rights will depend on their role. As described in earlier sections, the original administration rights are borne on the CIWIN Executives. The Executives will have access to a set of administrative rights. First, the Executives right to add new members is the core mechanism to enable a controlled extension of the CIWIN community.

***Requirement** 27**:** A CIWIN Executive can register CIP Officials of their country as members of the CIWIN system.*

The CIWIN Executives will have the ability to create new areas based on the types (see requirements 22 to 26) and assign CIWIN members to it.

***Requirement** 28**:** A CIWIN Executive can create new dynamic areas and setup their membership.*

The CIWIN Executives determine the access rights to the information provided by CIWIN members. The owners of the information placed in CIWIN propose access rights which are ultimately approved by the national CIWIN Executive. This applies principally to the document published in the library area, but can apply to all information produced by the country's CIWIN members.

***Requirement** 29**:** CIWIN Executive controls CIP information made available outside his Member State.*

Practically, as the CIWIN membership increases, the administrative rights held by the Executives may need to be delegated to national authorities. It will be up to the CIWIN Executives to delegate their administration rights to the appropriate organisation departments.

***Requirement** 30**:** CIWIN will allow delegation of the administration rights. The basic rights for CIWIN are the creation of new CIWIN members and the granting of CIWIN member's access rights to areas and documents. **Requirement** 31**:** CIWIN will record the expertise of the CIWIN members. The expertise level can be used as one of the parameters that determine the access rights to areas and discussion forums.*

1.7. No common trend on language of information exchanged through the system

Description

As the language used for discussion threads and one-to-one communication is chosen by each user, this question asked to the Member States deals essentially with the language of the documents to be uploaded. There is no agreement between the Member States on the language in which the information related to CIP is to be shared through the system.

Globally speaking, the choice of the Member States concerning the language used for the exchange of information through the system was inspired by two main concerns:

- *Concern for low barriers to make information available:* The purpose of the system is to make it possible to exchange CIP information with other users. As the exchange of information is on a voluntary basis, several Member States have stressed the fact that such exchange should be in a simple and straightforward way. A lot of national background information and documentation is however not available in all EU languages. Member States are concerned that -if such documents have to be (partly) translated- very few information will be made available by the users.

- *Concern for understanding information available:* With its current 27 Member States, the EU counts no less than 23 official languages. No single user can be expected to master all these languages. Thus, if no language policy is established for the system, users will not be able to understand all information made available on the system.

Taking these concerns in mind, none of the Member States has chosen the option of making information available in the language of the sender (owner) only.

The option of making information available in English only has been chosen by six countries as a first choice, and by a seventh country as a second choice. Reasons mentioned by these countries are that English is the language most often used by CIP experts and that the use of one common language helps to establish a common CIP vocabulary for the CIP community. It should be noted that many of these countries specifically mentioned that -if the option of only using English would not be withheld for the system- they would not favour a solution that allows only a limited number of languages in the system (e.g. English and French). The reason behind this is that they judge the knowledge of other languages than English not well-established enough through Europe, making that documents in these limited languages would not be understood anyway- just like any other EU language except English.

The option to upload an English language summary together with the full version of the information in the language of the sender (owner) was favoured by four countries. The reasoning behind this choice is that this option keeps the barrier low to make information available and that Member States are free to translate documents if -based on the summary- they deem the contents interesting enough. A comment made against this option was that a summary may not always reflect the entire contents of a document, thus making it possible to misjudge the relevance of this document. On top of that, not all countries have the necessary people and means to be able to summarise and translate documents from all EU languages to their national language.

The option of making it possible to upload information in any official EU language together with an English translation by the sender (owner) is favoured by seven countries as a first choice and two countries as a second choice. The arguments for this choice are that this option allows all EU languages to be represented in the system and that users not able to understand e.g. English would still be able to consult information made available in their language. A comment made against this option is that it would raise the barrier to make information available.

The option foreseeing an automatic translation of information uploaded in any official EU language into the other languages was favoured by six countries as a first choice and three countries as a second choice. The reasons mentioned for this choice were to keep the burden to upload a document low and to grasp an idea on what a document is about. The main reason mentioned against this option was the poor quality of such automatic translations. Given the fact that the topic of the information shared in the system may imply a specific vocabulary, this problem of poor translations is expected to be even bigger.

Other language options favoured by a Member State were first of all to upload all information in English but make it optional to foresee a translation of the document in another language or to upload all information in English and foresee an automatic translation from English (only) to the other EU languages. The logic behind the latter option was that the country expected that most people would not need a translation and that –if translation would be needed- it would be easier to find software that allows for good quality translations from English to other languages than a software allowing translation from any EU language to another one.

In any case, the option chosen for the CIWIN system would have to correspond to the following additional needs expressed by the Member States:

- No matter what the choice is of language, the system should allow that different language versions are made available for the same document. Although being different documents, the system should recognise these documents as being the same. So for example when search actions are performed, it should be made clear to the user which search results are different language versions of the same document and which ones are not.

- No matter what the choice is of language, the system should allow documents to be made available in any language if the receivers for the information belong to a restricted group. This could for example be the case for a collaborative work space created for several CIP experts within one country. (see also 'Ways to share information through the system')

Implications for the CIWIN system

The translation of documents topic applies mainly to the documents held in the CIWIN repository (library area) and the news bulletins. The use of language in the discussion groups and peer to peer communication will be determined by the users themselves and the terms of use of the system.

The CIWIN system infrastructure will support all Member State languages.

Requirement 32*: the CIWIN system functions must be accessible in all the Member States' official languages currently in use.*

Concerning the library, CIWIN will support translated versions of key information, without enforcing it. The translation requirements applicable to the document library are:

Requirement 33*: It must be possible to attach one or more translations of content to a document. As the translations can be produced by different methods providing varying degrees or reliability, there must be an indication of the translation's quality and reliability. CIWIN must also support a process for attaching translation with the proper approvals.*

The indication will enable users to distinguish formal/official, casual and automatic translations of the document content.

1.8. Positions regarding ways to share information through the system

Description

There are different ways to exchange information regarding CIP through the system. The Member States were asked to give their view on exchanging information through a document library, discussion threads, message boards, one-to-one communication and collaborative work spaces.

Document library and web links

All countries are in favour of making information available through uploading documents to the platform. As described above, several Member States have expressed the wish to avoid duplication of information already available on the internet by providing external links to the web sites concerned.

Discussion threads

Four countries are not in favour of foreseeing discussion threads in the system. The reasons mentioned for their choices were:

- *No added value:* the members of the CIP community already share views with each other on a regular basis during conferences, European level working groups or by e-mail and telephone. Especially countries not in favour of granting access to a large community of CIP experts hold this position.

- *Security concerns:* as discussed above, some countries fear that users posting comments as a reaction on discussion threads may make some sensitive or classified information available to other users. By not foreseeing discussion threads, the risk of such security breaches through human error is avoided.

- *Time constraints of CIWIN users:* The CIWIN users will exchange information through the system next to their daily tasks. The experience with discussion threads on national systems has shown that there is no real need to foresee such functionality as most users do not use it.

The other countries are in favour of discussion threads on the system. Depending on the country, discussion threads are rather seen as a way to exchange information or as a way to get to higher quality knowledge. Moreover there is agreement on the need to foresee both sector-specific and cross-sector discussion forums. Eleven countries are also in favour of sub-sector discussion threads, although some made the comment that the relevance of such forums depends on the sub-sector and that they may be set up in a next step of the implementation of the system.

Following the general differences in approach regarding the standard rights attributed to different users of the system, the Member States have different approaches on who should be given access to these discussion threads and what rights (read/write) the users should be given. Some Member States prefer giving reading and some even writing rights to all users of the system for each forum, whereas others prefer to limit these rights to communities on a "need to know" basis.

Message board

The main difference between discussion threads and a message board is that the latter is designed for one-way communication, whereas a discussion thread allows for authorised users to reply to a message and read all reactions from other users on the original and subsequent messages. Taking this into account, a message posted in a message board may however contain contact information, allowing subsequent communications on a one-to-one basis (e.g. through e-mail).

In general, all Member States but two were not opposed to a message board to post CIP news (e.g. "Proposal for Directive accepted by the Council") and information on CIP events (e.g. CIP conferences) on the system. Twenty-one countries saw an interest in making information on CIP events available, whereas seventeen countries saw an interest in putting CIP news on the message board. Most countries however indicated a low priority for such functionality in the system.

It should be noted that some of the countries not in favour of discussion threads do see a role in such a message board to take over some of the functions of a discussion thread. A user could

in their eyes request for certain information on a message board. Any subsequent communication could then take place on a bilateral basis.

One-to-one communication

Within the CIWIN context, one-to-one communication is generally understood as a (secure) e-mail functionality built within the system. Generally speaking, a considerable group of seven countries is not in favour of such functionality for the system. The main reasons for this objection are:

- *One-to-one communication is already possible outside the system:* Member States already exchange information (classified or not) with each other through e-mail. If needed, these e-mails are encrypted.

- *Some Member States want to keep control over the information flow from their country:* As mentioned above, some Member States are very keen on keeping control over any information related to CIP leaving their country. The reasons behind this request for control are the fear for security breaches through human errors and the fact that some CIWIN Executives prefer to keep control over all cross-border communication from their country.

- *Lack of Member States' trust that such CIWIN e-mail functionality will be secure:* As Member States do not have a detailed view on the security measures put in place for the system, they will prefer other ways to exchange sensitive information with each other.

- *Legal implications of sending and receiving information:* As mentioned above, some Member States mentioned legal implications of civil servants sending and receiving information, such as the obligation to share this information with the press if the latter requests this.

The other countries are in favour of such a functionality for the system, but attribute a low priority to the need. Additional comments made by these countries are:

- *Need for one-to-one communication between Member States:* Next to the general cross-European sharing of information the Member States expressed a need to be able to exchange information on a bilateral basis.

- *Need for one-to-one communication within the Member States:* for those countries who wish that the system will also be used for the exchange of information between users within their country, such an e-mail functionality is another way of achieving this goal.

- *Security measures are needed:* Access to such mailboxes should be clearly defined as classified information may be exchanged in this way. Additionally, as the users may not be permanently logged into the system, there should be a way of informing them that they have an e-mail message in the system, without disclosing the contents of the e-mail itself.

Restricted spaces for collaboration

Restricted spaces for collaboration allow a limited group of authorised users to share documents with each other, have internal discussions (discussion threads), post messages which can only be viewed by those with access to the restricted space etc. In addition, they

allow for several users to contribute to a document without any unauthorised user having access to this working document.

One country preferred to see a prototype of the system before answering on this question. Four countries are not in favour of such restricted collaborative work spaces in the system. The main reasons are:

- *Such collaboration is already possible outside the system:* Some Member States say they already collaborate with other Member States outside the system. They do not see a need for the system to foresee such functionality and think that it will not be used.

- *Some Member States want to keep control over the information flow from their country:* As mentioned above, some Member States are very keen on keeping control over any information related to CIP leaving their country. The reasons behind this request for control are the fear for security breaches through human errors and the fact that some CIWIN Executives want to monitor all cross-border communication from their country.

- *No need to limit access in a system with restricted accessibility:* This argument is in line with the position of some Member States that -once a user is granted access to the system - the rights of a user should not be further limited.

The other countries are in favour of a restricted space in the system, although it should be mentioned that five countries give a medium to low priority for this functionality. The types of communities that might be interested in such a collaborative work space are according to the Member States:

- Users within a country

- Users from a limited group of countries (e.g. Nordic states, Baltic states,…)

- Cross-European users from one or several sector(s)

- Cross-European users part of the same EU expert group

It should however be noticed that some countries are keen on avoiding collaborative work spaces for their national users through the CIWIN system as it would duplicate functions of existing national systems.

Implications for the CIWIN system

Taking into account the input received from the Member States, the first set of requirements list the information exchange mechanisms that will be supported by CIWIN:

Requirement 34***:*** *CIWIN will provide a library of CIP generic documents such as best practices. The access to the library will be subject to access control right based on the "need-to-know" principle.*

Requirement 35 *[optional]: CIWIN will provide discussion forum capabilities for multi member discussions. The access to the discussions will be subject to access control right based on the "need-to-know" principle.*

Requirement 36 *[optional]: CIWIN will provide news bulletin boards capabilities for communicating information to CIWIN users. The access to the news bulletin boards will be subject to access control rights based on the "need-to-know" principle.*

Requirement 37 *[optional]: CIWIN will provide a mechanism allowing CIWIN members to exchange private messages (email). The email functionality will be limited to the CIWIN system.*

Requirement 38: *[optional]: CIWIN will provide a mechanism allowing CIWIN member to exchange private instant messages ("chat").*

The need for restricted spaces is covered by the concept of specific topic areas (see requirement 22).

1.9. Other functionalities of the system

Description

Search functions

The question regarding the preferred search possibilities of the system is very closely related to the actual language solution that will be decided upon. Depending on whether or not documents will be made available in one, several or all languages of the EU, certain search possibilities gain or loose their relevance.

Ten Member States indicated all search possibilities as interesting, suggesting that users should be able to choose the way of searching they prefer. Next to this finding, the searching with full text is clearly preferred (all countries except for two) in comparison to searching based on just key words (seventeen countries). The main reason why some countries are not in favour of searching based on key words only is that they fear that this would require the indication of all these key words when uploading documents. Searching through a multi-lingual thesaurus (similar to EUROVOC) is favoured by eleven countries.

Reference list of documents not visible

During one of the pilot interviews it was suggested by a country to foresee a reference list of documents which can not be directly downloaded from the system but which could be obtained from the document owner directly upon request.(if he/she approves). Three countries are not in favour of foreseeing such a reference list. The main reasons for this are the practical burden of answering all these e-mails and the principle that if a user is not authorised to certain types of information, it would be better not to show the information in the first place.

The other countries are not against such a reference list, but some indicate a low priority for such functionality. Member States in favour of this functionality believe that it is a tool that allows the Member State to control the flow of information and that it may enhance the trust of countries to put information on the platform.

Metadata

Metadata are data about data - more specifically information (data) about a particular content (data). An item of metadata may describe an individual datum (content item) or a collection of data (content items). Metadata is used to facilitate the understanding, use and management of

data. In the context of an information system like CIWIN, where the data is the content of the computer files, metadata about an individual data item might typically include the name of the file, the type of file and the name of the data administrator.

Member States were asked to indicate the metadata they find most important and those they would consider as mandatory when uploading documents to the system. Generally speaking, there are no big differences between the answers. The EU countries expect a sophisticated search ability of the system, while keeping the barrier of uploading information as low as possible. Concerning the mandatory fields; few countries indicate mandatory fields, whereas others explicitly ask to avoid mandatory fields because they fear that it would create an additional barrier for users of the system uploading documents.

Concerning the actual metadata, the *'document date'* is most favoured (Twenty-one Member States, four indications as mandatory). Several countries also formulated the need for an indication of when the information in the document can be considered to be obsolete. Also the *'security classification of the document'* is highly favoured as metadata (twenty MS, three indications of mandatory). Countries not in favour of such metadata are those that do not wish or expect to exchange any classified information through the system. Next follows the *'author's name'* (nineteen Member States, three indications as mandatory), but some countries see this rather as the name of the document owner, which could be the name of a national unit or department, rather than the name of an individual.

The countries were also asked whether or not they were in favour of adding '*traffic light information*' to documents when uploading information. This indication can be used to give guidelines to the receiver of unclassified information on how to treat the information. 'White' information may be freely distributed to any person, 'green' information to all users of the systems, 'orange' information to those with a "need to know", whereas 'red' information is shared on a one-to-one basis. With the exception of five countries, most Member States are not opposed to such a protocol. However, only one country sees it as mandatory information. Those in favour of a traffic light protocol find that it gives a clear indication of how users should treat the information and that it allows differentiating non-sensitive unclassified information from sensitive unclassified information. Those not in favour argue that it creates unnecessary complexity in indicating the sensitivity of information ("information is either classified or not, not something in between"), or do not wish or expect to share any sensitive information through the system in any case.

A few Member States also requested the possibility to indicate the importance of a document (e.g. adding a 'red flag' to a document)

Notification of new contents on the system

Platforms for information exchange may allow for certain types of notification of the users to inform them that information has been added or updated in the system. Such notification could deal with new documents uploaded, but also with new discussion threads, new information on the message board etc. Three Member States are not in favour of any type of notification as they start from the principle that users will check the system regularly if indeed they find the information put on it interesting.

In order of preference of the Member States, the most requested types of notifications are: customised e-mail notification (seventeen Member States), RSS feeds (eleven countries),

monthly summary newsletters (ten countries) and weekly summary newsletters (nine countries). Next to this, the Member States also request:

- A sophisticated level of customisation of notification, making it possible for every user to clearly indicate which types of information he/she is interested in being informed of.

- When a user logs in, the system should show a (customised) summary of the updates of the information on the system since the last time that the user has logged in

- Notifications should be foreseen with special measures to ensure the security and sensitivity of the information in the system. This means for example that the new or updated information should not be sent to e-mail addresses external to the system.

- Notifications should indicate which updates are of the highest importance

Facilitation of organisation of meetings and trainings

The countries were asked whether they were interested in a functionality facilitating the organisation of meetings and trainings (regular, phone or video conference) -involving the invitation of participants, tracking the response to meeting requests, a notification of participation, the upload of relevant documents, etc.

Generally speaking, this feature is not in high demand. A considerable group of eleven countries is not in favour of this functionality and those in favour of the feature indicate a low priority ("why not?"). The main reasons for the low demand for this feature are:

- *Existing alternatives for these functions:* there are currently already different ways in place for organising meetings with participants from across the EU. Member States want to avoid the system to contain any duplication with existing ways of working.

- *Focus the functionalities of the system to its core tasks:* the core task of the system is to exchange information related to CIP, not to facilitate the organisation of meetings. Therefore, such a feature is not needed in the system.

- *No need for such functionality.* There is no business need for such functionality. Therefore, it will not be used.

As Europol is currently in the process of setting up a tool to facilitate the organisation of meetings with participants from across Europe, one Member State suggested to wait with the implementation of this functionality in the CIWIN system and to learn from the Europol experience.

Additional questions from the Member States

Next to the answers to the questions mentioned in the Interview Guide, the Member States were also invited to inform the study team of additional features they might deem interesting for the CIWIN system. Generally speaking, most countries *requested to be shown the prototype of the system* and some examples of information that would typically be shared through the system. Based on that information, the Member States expect to come up with additional recommendations regarding the system.

Next to that, one Member State suggested to foresee a *Wiki-functionality* for the system, as it would allow the CIP experts to create a common knowledge encyclopaedia related to CIP on the system. Such type of functionality is also foreseen in the Finnish national system, which -amongst others- allows for the exchange of CIP related information between national civil servants.

MS also request clarity regarding the hosting of the system and whether or not the data will be stored in a central database or in several databases (e.g. one in each Member State). It is also requested that the CIWIN system would be made available on a stable platform, with excellent availability. Several Member States mentioned that the current TESTA network does not fulfil this need. Information on these matters will define the trust the Member States will have in the new system.

Implications for the CIWIN system

These functions will be provided by CIWIN as far as the further functionalities of the system are concerned:

***Requirement** 39**:** CIWIN will provide state of the art search functions to locate information held within the system. The search will always limit the search to the information accessible by the user. The search will allow structured search based on document indexing information and unstructured search for content document specific patterns.*

***Requirement** 40**:** The CIWIN search system will support multiple languages*

***Requirement** 41**:** The access rights to a document must include the ability to view the document in lists.*

***Requirement** 42**:** The CIWIN system must allow indexing of documents (meta data). The indexing of document can be optional. Usage will determine whether or not indexing should be enforced and for which metadata items.*

The scope and definition of metadata will be analysed during the construction of the prototype.

***Requirement** 43: The CIWIN system will provide a calendar feature that will allow the coordination of activities and events within areas.*

***Requirement** 44**:** The CIWIN system will provide a notification mechanism that will allow users to determine document updates or events that will issue notification messages.*

CIWIN will provide wiki-functionality for enabling collaborative authoring of documents. This functionality is initially foreseen in the Expert Working Group areas for the authoring of best practices and working group artefacts.

***Requirement** 45: [optional]: CIWIN will provide wiki-functinality for collaborative authoring of CIWIN content..*

2. Main findings concerning a rapid alert functionality for CIWIN

In the Commission Communication regarding the European Programme on Critical Infrastructure Protection, it is mentioned that the CIWIN system will provide an optional

platform for the exchange of rapid alerts. A rapid alert system (RAS) is a system that allows for the rapid distribution of information regarding a threat or an event (first and subsequent messages) to the relevant receivers with the purpose to allow the receivers to take well-founded time-sensitive actions and/or decisions.

In order to perform this function, a rapid alert system may support its users by providing several functions. These functions may entail the following:

- *Detection and analysis:* Rapid alert systems may allow for early event detection through the rapid reporting of cases that may lead to the type of emergencies covered by the RAS. The analysis may take place by some users of the system who subsequently share their findings. It may also happen collectively, e.g. by using the system itself. Functionalities may be integrated in the RAS to simulate the effects of the event to ensure a rapid, smooth awareness of the impact of what has happened.

- *Alerting:* Rapid alert systems typically allow for the distribution of an alert through one or several communication channels to all relevant recipients. The sending of an alert is usually preceded by a certain way of risk assessment and may be preceded by a formal approval by the relevant authority. Who should be receiving the alert in what type of situation is determined according to a predefined business logic. Recipients of the information may have to authenticate themselves and/or acknowledge reception of the message.

- *Response:* Rapid alert systems are designed to facilitate a time-sensitive action and/or decision by its users. Once the alert information is distributed, the system may further support the subsequent (joint) actions and decisions. This could be done by simply making the information available in the system to consequence managers, or this may be done in more sophisticated ways by providing decision support tools.

Once a crisis has taken place, the users of the rapid alert systems may want to examine the events that happened and the subsequent actions taken in order to learn from the event and generate e.g. best practices. By logging the inflow of information and the actions of the users, a RAS may support such examination exercises.

Rapid alert systems –especially those used at an international level- often have a set of standards-based vocabulary (which may be multi-lingual or not) with clear definitions for the users and users have rules and procedures regulating how and when to use the system. Due to their nature, rapid alert systems are made available on robust platforms and are operated on a permanent basis (24/7 availability).

2.1. The majority of the Member States is in favour of a Rapid Alert functionality for CIWIN

Description

Although there are eight countries that want to opt out on this functionality for the system, seventeen countries have expressed an interest in providing a RAS for CIWIN.

Countries not in favour of a RAS

Eight countries are not in favour of a rapid alert functionality for CIWIN. The main reasons for their objection mentioned are:

- *The added value of a CIWIN RAS compared to the existing European RAS is unclear:* Many European-wide RAS already exist, covering several sectors and sub-sectors which are part of EPCIP. If there are (sub-) sectors that are currently not covered by existing European-wide RAS, these countries suggest extending the existing RAS instead of building a new system.

- *The consequence managers already dispose of a RAS:* This argument is closely related to the previous point, but is highlighted as many Member States made this comment. It boils down to the fact that Member States see the civil protection forces as the main consequence managers responsible to act if a crisis takes place related to a critical infrastructure. In case of crisis, the actions of the civil protection forces are coordinated in the national crisis centres, which are connected to the CECIS system. If there is any additional information to be exchanged between these consequence managers which is currently not possible through the CECIS system, it is recommended to extend the functionalities of that system instead of building a new system.

- *Avoid any duplication of national competences:* The suggestion that a CIWIN RAS might directly alert owners and operators of critical infrastructures is seen as a duplication of the national competence to inform these actors in case of a serious event. In some countries this notification happens through national rapid alert systems.

- *Temporary opt-out to see how the RAS would work:* Some Member States have mentioned that for the time being they prefer to opt out of the rapid alert functionality as it is not clear to them what type of information would be exchanged and in which type of events the system would be used. Once the system is put into place, they will re-evaluate their position on the matter.

- *Reluctance to share intelligence information through CIWIN RAS:* As the EPCIP programme is based on an all-hazards approach, some countries fear that intelligence information regarding terrorist threats may be exchanged through the system. Some countries are against sharing intelligence information through the CIWIN RAS as there already exist channels to exchange such information (e.g. Bureaux de Liaison - the BdL network) and as this entails security levels not envisaged for the CIWIN system.

- *Cross-sector characteristic of EPCIP:* As the EPCIP sectors are very diverse, the competences to deal with crises in those areas are very much split up as well. Some Member States feel that for this reason it does not make sense to build one system that would cover all these sectors.

Countries in favour of a RAS

Seventeen countries are in favour of a RAS for CIWIN. However, not all countries in favour of such RAS functionality see this is a high priority. Next to this, some additional concerns and remarks were also made by this group of countries:

- *Relationship between CIWIN RAS and existing European-wide RAS:* Member States request clarity on the relationship between the CIWIN RAS and existing European-wide RAS, as they feel that (part of) the functions and (part of) the sectors that would be covered by the CIWIN system are already dealt with by the existing systems. The part describing the different views on the CIWIN functions and relationship with other systems deals with this question in further detail.

- *Question on mandatory versus voluntary exchange of information:* A few countries requested clarification on whether or not the exchange of rapid alerts through the system should be on a mandatory or rather voluntary basis. For example, the Meridian rapid alert network operates on a voluntary basis, with peer pressure as the main driver for quality. Some Member States prefer the CIWIN RAS to be operated according to the same principle.

- *Relevance of RAS depends on the (sub-) sector involved:* Even if some Member States have no objection against RAS functionality for the system in principle, they have mentioned that the relevance of a RAS may not be as high for all (sub-) sectors involved in the EPCIP programme. A case-by-case evaluation for each sector would be welcomed by these Member States.

Implication for the CIWIN system

For the Member States interested, the CIWIN system will include a rapid alert function

***Requirement** 46: The CIWIN system will include a RAS functionality to enable the rapid distribution of information regarding a threat or an event (first and subsequent messages) to the relevant receivers with the purpose to allow the receivers to take well-founded time-sensitive actions and/or decisions.*

2.2. There are different views on the functions of the CIWIN RAS and its relationship with existing RAS.

Description

The missions to the Member States made it clear that they have different views on the functions they expect the CIWIN RAS to perform and on how the system will be integrated in the existing framework of European and international RASs.

Different views on functions of the CIWIN RAS

The Member States request some clarification of what type of RAS functions the CIWIN RAS will perform. Although this was not always articulated in an explicit way, Member States have different interpretations of which RAS functions (as mentioned in the introduction) the CIWIN RAS is expected to fulfil and more specifically on whether or not the CIWIN RAS should perform the task of detection as well.

- *Vision of the CIWIN RAS as performing detection, alerting and response functions:* Although an important part of the detection function is typically performed by the Member States, some cross-European systems assist in collecting information from these countries in order to create a pan-European overview of a situation, allowing for analysis of ongoing trends. An example of such a system is EURDEP (EUropean Radiological Data Exchange Platform). Also the CERT network performs similar functions. In this view, the CIWIN RAS is seen as a system in which a certain exchange routine is established on events taking place concerning critical infrastructures in Europe. Based on the cross-European analysis of such routine information cross-European trends may be identified which may lead to the launching of an alert. Also in the occurrence of a serious event it may be decided - according to predefined criteria- to launch an alert to inform the relevant recipients. Subsequently the response phase takes place.

- *Vision of the CIWIN RAS as performing alerting and response functions only:* This vision sees the CIWIN RAS as a RAS serving to distribute information regarding serious events only. Typically the task of detection (and a part of analysis) is performed outside of the system by other systems and/or networks. Specific and technical information is thus not initially collected in the system, but may have to be transferred to it once it is decided - according to predefined criteria- to launch an alert to inform the relevant recipients. Depending on the objective of the RAS, information spread through the system may be specific and technical or rather generic. Subsequent to the alert, the response phase takes place.

Each of these visions on the CIWIN RAS functions has its implications on how the CIWIN RAS will relate to the existing European and international RAS.

Relationship CIWIN RAS and existing European and international RAS

The cross-sector nature of the EPCIP programme makes that many Member States ask the question on how the CIWIN system will interact with other existing European and international RAS which perform (certain) rapid alert functions for specific (sub-) sectors.

Different RAS currently exist at the European level. Some of these RAS deal with emergencies regarding specific topics (e.g. EWRS on communicable diseases, ECURIE on radiological emergencies, RASFF on consumer health in relation to food and feed, etc.), whereas others deal with specific dimensions of crisis. (e.g. CECIS to assist Member States in coordinating their response to a crisis)

Next to these existing RAS at the European level, several RAS also exist on the international level. The CERT network for example addresses risks at the software and system level. Although it was established as an incident response team, the CERT Coordination Centre has evolved beyond that, focusing instead on identifying and addressing existing and potential threats, notifying system administrators and other technical personnel of these threats, and coordinating with vendors and incident response teams world wide to address the threats. Another example is the GDACS (Global Disaster Alert and Coordination System) which provides near real-time alerts about natural disasters around the world and tools to facilitate response coordination, including media monitoring, map catalogues and a virtual on-site operations coordination centre. The Member States also referred to the NATO Intelligence and Warning System (NIWS) which covers threats to NATO, as well as a wide variety of military and non-military risk indicators.

If the CIWIN RAS is to perform detection and/or alerting functions for all of the sectors and sub-sectors mentioned in EPCIP, the system will have to find a way to relate to the existing rapid alert systems. Avoiding any duplication of tasks performed by existing systems is key in this respect according to the Member States.

- *CIWIN RAS performing detection functions:* If the CIWIN RAS will have as one of its tasks the regular collection of information regarding events (major and not) related to critical infrastructure, it has to avoid duplication with any such information collection by other systems. Whereas the detection function is mostly performed by the MS, some European and international systems also perform this task. Examples mentioned by the MS are the CERT network, EURDEP (EUropean Radiological Data Exchange Platform) and – to a certain extent- EWRS (communicable diseases). Therefore, when relevant, there should be a way to introduce information from other existing systems into the CIWIN

system. MS want to avoid that they will have to input the same information into different systems. For those (sub-) sectors for which does not exist a European or international system to fulfil the detection function, it may have to be evaluated whether or not there is a need for such a function or whether this should rather remain entirely at the national level.

- *CIWIN RAS as performing an alerting function:* If the CIWIN RAS will have as one of its tasks the distribution of rapid alert messages to the relevant recipients, it has -according to the Member States - to avoid duplication with any such information sent around by other systems. Several sector-specific rapid alert systems already exist at the European and international level, such as ECURIE[9]. The Member States request clarity on whether or not the CIWIN system will perform rapid alert functions for these sectors as well. If this is indeed the case, the Member States want clarification on what type of information will be sent through the CIWIN system and to what extent this would be different from the existing systems. The EU countries want to avoid that they will have to input the same information into different systems and also that they will receive the same information through several systems. This concern is very concrete as several Member States indicated that they expect the CIWIN RAS to be operated from their national crisis centre, in which the entry point of other European RAS is also located. On the other hand, if sector-specific information is needed in CIWIN, the users of the sector RAS might be best placed to input/receive this information.

Although of a different nature and purpose than the sector-specific RAS, the ARGUS system plays an important role in case of major multi-sector crises, supporting the response by the Commission services. The Member States request some clarification on how the ARGUS system will be related to the CIWIN system.

Implication for the CIWIN system

The CIWIN RAS will provide the means to communicate alerts to the CIP community accessible via CIWIN, and collect notification acknowledgements.

***Requirement** 47: The CIWIN RAS system will enable structured exchange of CIP alerts and leverage the CIWIN's CIP contacts list to ensure the distribution of alert notifications to the CIWIN contact based on the nature, importance and scope of the alert.*

The CIWIN RAS will therefore provide an optional structured inter-state media for exchanging CIP alerts. The alerts intended to be suitable for CIWIN are those derived from the analysis of detailed alerts provided by specialised RAS systems and their operational alert monitoring staff. The processed information nature of the CIWIN alerts differentiates them from those produced by other rapid alert systems. For this reason, there is no compelling reason to envisage, at least in its initial deployment, connections to other RAS systems to automatically collect alerts relevant to CIP. The generation of alerts will therefore be achieved through manual entry of the alert information into the CIWIN RAS.

2.3. Those countries in favour of CIWIN RAS hold different views on the security level of the CIWIN RAS

Description

Although only one country in favour of the CIWIN RAS specifically mentioned the fact that the CIWIN RAS would be accredited up to the level of EU restricted as an added value of this system, it is clear from the Member States' answers that special security measures are

expected for the system. Having said this, the Member States have different opinions on the maximum level of security classification of the information that should be exchanged through the CIWIN RAS. Ten countries in favour of the RAS expect that the system would allow for the exchange of information up to the level of EU restricted. Four countries expect the system to allow for the exchange of information up to the level of EU confidential. With the exception of one country, these countries also requested the CIWIN forum to allow for information exchange up to this security level. Finally, one country requested a level of EU secret, whereas another country requested the level of EU top secret.

Although a considerable group of Member States would find the level of EU restricted satisfactory for the system, it is apparent that there are divergent views on the likeliness of the level of classification of the information that will be exchanged through the system. This difference may follow from the fact that the system will deal with both threats and events, from different interpretations of the contents of a threat message, from the all-hazards approach of EPCIP which includes terrorism and from different interpretations of what the security levels entail:

- *Different security levels for threat information versus information regarding a catastrophic event:* In principle a RAS can be used for the distribution of information about threats and about catastrophic events. But some countries may expect the system to be used mainly for threats, whereas others expect it to be mainly used for events. Information that a catastrophic event has occurred may not necessitate a high security level as this type of information is rapidly spread through the media etc. Information regarding a (perceived) threat is however much less publicly known and may have to be treated in a more secure way.

- *Different interpretations of the term "threat information" and its implications:* Whereas in some countries a threat may be a loose indication that something might be happening, in other countries a threat is referred to as specific information which has been confirmed by intelligence services. In some countries threat information is distributed on almost a daily basis, whereas in other countries this is very exceptional. In some countries sending inaccurate threat information to owners and operators of infrastructures may lead to claims for compensation, whereas this is not the case in other countries. This difference in interpretation leads to different ways to treat the information. Whereas intelligence based information has to be treated with high security measures, this may not have to be the case for more general threat information.

- *All-hazards approach, including terrorism:* As already mentioned for the CIWIN forum functionality, the general approach of the EPCIP programme is to protect critical infrastructures against all types of disruption or destruction, ranging from a natural event to a human-caused accident to a terrorist attack. As terrorism is thus included in EPCIP, some countries may expect that information regarding terrorist threats will also be exchanged through the system. Such information, often intelligence-based, requests high security levels.

- *Different interpretations of security levels:* Although the security levels mentioned in the Interview Guide of the missions have been clearly defined at the European level, it should not be excluded that the people met in the Member States may have different interpretations or are not (fully) aware of the required security measures for each classification level, both concerning the system itself and its users.

Implication for the CIWIN system

There is no doubt that the security level of the CIWIN RAS constitutes a controversial issue as far as the Member States are concerned. In order to respect the different national views without putting in danger the security of the CIWIN RAS, the following possibility will be implemented: the alert information will be considered from an access control point of view in the same way as any other information held in CIWIN and the basic access right rules will apply.

***Requirement** 48: The access to CIWIN alerts will be governed by the same need-to-know rules that control the access to any information held in CIWIN.*

2.4. Those countries in favour of the CIWIN RAS hold different views on the user community of the CIWIN RAS

Description

A rapid alert system allows for the rapid distribution of information regarding a threat or an event (first and subsequent messages) to the relevant receivers with the purpose to allow these receivers to take well-founded time-sensitive actions and/or decisions. In terms of defining the CIWIN RAS community, it is thus important to know which actors the Member States see as senders and receivers of alerts. It is equally important to define the communication tools through which the alert messages will be sent.

Senders of alerts through the system

As mentioned earlier, the countries differ in the degree to which they actively involve the owners and operators of the CI in the policy making and actions concerning CIP. Despite these differences, almost all countries in favour of the CIWIN RAS see the senders of the alerts through the system to be the members of the European and national administrations and not the owners and operators of the CI. Only two countries were in favour of granting such rights to owners and operators of critical infrastructures. There was no difference in the answers depending on whether the owners and operators are private or semi-governmental (e.g. state enterprises) or whether the owners and operators are located within a country or are rather situated at the European level (e.g. Galileo). A few countries mentioned that –once the system is successfully operational for a while- granting alert sending rights to the owners and operators of critical infrastructures might be taken into consideration again.

Two countries did not indicate the European Commission as a possible sender of alerts. This could indicate that they see the detection, evaluation and subsequent sending of alerts as a Member State's responsibility.

The Member States have different views on the level at which alert sending rights may be distributed within their national administrations. All Member States agree that the CIP contact points should be allowed to send alerts through the system. In only six countries the officials of the administrations responsible for the different (sub-) sectors may also be allowed to hold alert sending rights. The main reasons why most countries prefer not to delegate such rights to officials responsible for the (sub-) sectors are that they prefer to keep control over the alert messages sent from their country and the practical fact that there is no permanence of duty in all those ministries/departments/units responsible for the different sectors. Of those countries allowing administrations to send alerts, only two would allow these administrations to send the

alerts directly, whereas the other countries would expect some kind of validation of the alert message before broadcasting it at a European level.

Next to these findings, some additional comments were made by the MS regarding their answers:

- *The 'CIP contact point' has to be interpreted in a flexible way:* Although the CIP contact person is seen as holding the official authority to approve the sending of CIP alerts, this does not necessarily mean that he/she always has to be the actual sender of such alerts. Given the inherent nature of a RAS, such a system has to be manned on a permanent basis. In some countries the body responsible for CIP coordination does not have a permanent service. Therefore, the actual sender of such alerts may for example be located in the national crisis management centre. Next to that, some countries indicated that they envisage nominating an entire unit as the CIP contact point, meaning that several persons may fulfil this function within a country.

- *Case by case evaluation of granting administrations responsible for (sub-) sectors, alert sending rights:* Some of the countries in favour of granting alert sending rights to the administrations responsible for the (sub-) sectors mentioned that –depending on the actual sector involved- such authority will be attributed on a case by case evaluation. For some sectors, granting such alert sending rights to the administrations makes more sense than for others.

- *The administrations responsible for (sub-) sectors may not always be located on the national level:* As some countries have a federal state structure, the authorities responsible for certain (sub-) sectors may not be part of the national level but are located at the sub-national level.

- *Commission sends alerts regarding European-level critical infrastructures:* Some countries suggested that the European Commission would be responsible for sending alerts regarding events taking place at European-level critical infrastructures (e.g. Galileo).

Receivers of alert information sent through the system

Almost all countries in favour of the CIWIN RAS see the receivers of the alerts through the system to be the members of the European and national administrations and not the owners and operators of the CI. Only two countries were in favour of granting such rights to owners and operators of critical infrastructures. All countries in favour of the RAS expect the CIP contact points to receive alerts related to CIP. Nine countries are in favour of the administrations responsible for the (sub-) sectors to also receive alert information next to the CIP contact point. However, the concern was expressed that the system should avoid sending all types of alert messages to all types of receivers. It is therefore seen as detrimental for the system that it would have sophisticated contact management software. The CIP contact point and the administrations responsible for the (sub-) sectors are seen as the key points to further distribute CIP alert information to the relevant actors within their countries.

Communication tools used for alert messages

Alert messages are put into the system by authorised users. Rapid alert systems may provide for several communication means to reach those indicated as authorised recipients of alert messages, such as fixed phone, mobile phone, e-mail, a radio network or simply through the

system. The contents of the alert messages should be concrete and concise whilst respecting the security classification of the message.

There is no outspoken tendency in opinion between those Member States in favour of a RAS functionality on what would be the best communication means to reach the recipients. The options most indicated by Member States were alerting through the CIWIN system itself and through an e-mail to a functional mailbox. For both options, most countries were in favour, with the exception of four countries opposed to alerting through the system and four countries opposed to alerting by e-mail to a functional mailbox. It should be noted that both of these options include the organisational necessity that there is a permanence of service foreseen for the recipients of the alert messages, i.e. a 24/7 manning of the computer on which the information will arrive. Significantly fewer countries are in favour of receiving alert messages in individual mailboxes (eight countries) or by mobile or fixed telephone (six countries). Only one country was in favour of receiving alert messages through radio.

Implications for the CIWIN system

In order to address the issue of who can launch an alert in CIWIN RAS, the CIWIN system must include the role of "alert sender" that will allow privileged CIWIN members to submit alerts to the CIWIN RAS.

***Requirement** 49: The CIWIN system must have a specific role for sending alerts.*

The assignment of this role to a CIWIN member would be done by the country CIWIN Executive (or his delegate).

Concerning the receivers of the alerts, the CIWIN system will support two complementary methods for their specification:

***Requirement** 50: The CIWIN system can automatically determine the list of alert receivers based on the alert characteristics and the information in the CIWIN contact list.*

***Requirement** 51: The CIWIN alert sender can specify a list of contacts that must be notified.*

In both cases, the CIWIN system must track the acknowledgements.

***Requirement** 52: The CIWIN alert sender must be able to know the acknowledgement status of his/her alert notifications.*

2.5. Expectations regarding information exchanged through the CIWIN RAS

Description

It is important that the alert message is quickly understood and accurately interpreted by those receiving the information. Some RAS use predefined fields which may contain a number of predefined values. Other RAS foresee free text fields or a combination of both. Given the cross-European nature of the CIWIN RAS, a solution concerning the use of languages will have to be defined for the system. Next to the automatic translation of predefined fields, several language options are possible, which are similar to those mentioned in the Forum part of the CIWIN system.

Given the cross-sector character of EPCIP and the CIWIN system, it is important to note that the type of alert information and the template used to communicate this information should be agreed upon by the Member States for each individual (sub-) sector, ideally for a number of possible scenarios. Rules and procedures will have to be agreed upon regarding the criteria to be used to select certain values of certain fields. Also the language option chosen may differ between alerts of different (sub-) sectors, as the user communities of the system may be different. Given the limited time and budget of the CIWIN project, it was decided that the Member States would be interrogated on their preferences regarding a generic alert message. For the actual CIWIN system, these findings will however have to be refined for each (sub-sector).

Generic alert message contents

Only two countries have indicated that certain fields should be mandatory. Most other countries stress the need to limit the number of mandatory fields for an alert message as in a crisis situation a lot of information may not be known or may be incoherent. It was also mentioned that crisis situations do not always match with the predefined scenarios, making it desirable to be flexible when it comes to filling out templates for information distribution.

Concerning the information contents of the generic alert message, all Member States in favour of the RAS agree on including the date of the event and its geographical location in the message. With some minor exceptions, there is also widespread agreement on including the local time of the incident/alert and the indication of the alert type (e.g. high/medium/low). Also widely approved fields are: the indication of the Member States originating the alert; background information on the alert preferably as free text; the Member State(s) potentially affected by the alert and an indication of the severity of the event, with for each two Member States that have not indicated the option. The field regarding the actions suggested to be taken by the Member States was least favoured by the EU countries, with only eight countries in favour.

Other information in RAS

Next to the information that the alert message should contain, some Member States have also indicated their expectations regarding other information that the RAS should allow to be exchanged. Such expected functionalities are:

- *The possibility to update information on an event once the alert has been sent.* As gradually more information becomes available regarding an incident, the originator of the alert message should be able to add information about the incident to the system, so that the other authorised users of the system have access to this information as well.

- *The possibility to make documents and external links available concerning the incident:* In order to quickly inform other authorised users of the CIWIN RAS of specific characteristics of the CI, the region it is located in, the authorities responsible etc, some Member States request to be able to upload documents or to provide web links in an accessible way.

- *Possibility to make contact details available:* Once an alert is launched, the sending country may want to make some contact details available of people responsible or experts.

- *A discussion forum on which the Member State experts may exchange information:* In case of crisis, there may be a need for CIP experts of the Member States to discuss matters with each other through the use of discussion threads. Once an alert is launched, such an alert-specific discussion forum should be made available. If possible, such discussion threads may sometimes be enriched with an attachment containing more detailed information of relevance to the alert under discussion.

- *Logging, archiving and review of crisis:* Once a crisis is finished, the Member States should be capable to review and –if needed- evaluate the past events and the actions taken. This can be done by a systematic logging of all information updates and actions taken during the crisis for later review. The archiving of all alert-specific information allows reviewing the events at any stage in the future.

Implications for the CIWIN system

The CIWIN system will allow two channels of communications on alerts. The RAS function itself will provide a formal channel for official alert information and updates provided by dedicated officials. The second channel of communication intends to allow the alert to optionally reach the larger CIP community to benefit from their experience for the matter at hand. This second channel will take the form of a CIWIN area dedicated to the alert. The alert area can be used to access the CIP experts and enable focused exchange of communication around the alert and management of its consequences.

***Requirement** 53: The CIWIN rapid alert system must enable the communication of official and structured information. It must be possible to communicate updates to the alert, and eventually close it.*

***Requirement** 54: The CIWIN system must enable the CIP experts to exchange information around a specific alert using a dedicated alert area.(see Requirement 25)*

The separation of the official and ad hoc information channels ensures the integrity of the official alert information and allows alert consequence managers to access the community of CIP experts for support on specific matters.

5.6. Interconnections of the CIWIN RAS with other RAS

Description

The Member States were asked to provide their opinion on possible interconnections through interface between the CIWIN RAS and other existing RAS, at the European, international and/or national levels. No country was fundamentally opposed to the principle to physically connect the CIWIN system to another system, as long as the necessary security requirements are met. Six countries answered no to the possible connection of the CIWIN system to other systems, but did so mainly for the reason that they did not have a national CIP system themselves which could be linked to the system.

In principle, the CIWIN system may in the eyes of the Member States be connected to any European or international system that collects similar information if this would mean that duplication of efforts to collect and distribute information is avoided. This being said, no single country indicated that it expects the CIWIN system to be physically interconnected to its national system at the moment of the start-up of the system. Some would refuse such a connection as a matter of principle, whereas others prefer to first evaluate the system once it is

set up, and to compare its set-up and data model with their national system before deciding on the matter. Member States however do foresee a human interface between the CIWIN RAS and their national RAS (if it exists) to transfer relevant information.

Those Member States willing to evaluate a possible interconnection between their national system and CIWIN once it has been made operational, are often concerned about the cost of building an interface between the national system and CIWIN.

ANNEX IV

CIWIN prototype's concept

The present document aims at describing the basic concepts of the CIWIN portal for the best understanding of its functioning. First of all, the roles of users are defined and described in this document. Secondly, this document gives a description of the different functionalities available in almost every area. A description of the various areas of the portal, enumerating the actors/roles active in each area, follows.

1. Roles

Hereafter are described the different roles that one person can have in the CIWIN system. According to the rights and responsibilities that individuals have in CIWIN, they could take on more than one role at the same time, e.g. they could be both the Editor and Approver of a document.

1.1. Administrator

The Administrator has full access to the administration portal for the configuration of the solution, and full control on all other parts for testing and maintenance reasons. What is more, the Administrator manages the requests for the creation of dynamic areas. He is in charge of creating the dynamic areas and removing unused or abandoned areas. The role of the Administrator will be dedicated to the Commission.

1.2. CIWIN Executive

The term "CIWIN Executive" refers to the CIP Contact Points nominated to represent their respective Member State in all issues related to CIP. The role of the CIWIN Executive is assigned to one representative per Member State and to one Commission Official nominated as the representative of the Commission. Each CIWIN Executive is also the Manager of his respective Member State Area. In his Managerial role, the CIWIN Executive has the ability to add and delete users, grant or deny access to any user for the Member State he is responsible for. What is more, the CIWIN Executive in his role as Member State Area manager will be the one enabling or disabling the optional Member State Area. The CIWIN Executive is able to delegate parts of his responsibilities to one or more national users.

1.3. Area Manager

The Manager has full control over an entire area. Full control includes permission management, people and group management and delegation. Having all these permissions for an entire area granted, the Manager is able to organise the area with full flexibility limited only by the available features as defined by the Administrator. Each CIP Contact Point is the manager of his respective Member State area.

1.4. Moderator

This role is assigned specifically and exclusively for the discussion forums in the portal. His task is to follow up ongoing discussions ensuring the consistency of them. He will be able to edit or remove posts that are not relevant, offensive or out of date.

1.5. Editor

An Editor is allowed to create new documents, specify their metadata, edit his own documents, participate in the creation of collaborative documents and modify those to which he has access. As contributor to a collaborative working document, an Editor is able to request its publication to the library. In order for a document to be available to a broader audience, it has to be approved for publishing by the Approver.

1.6. Approver

The Approver is in charge of reviewing the content and the metadata of a new document submitted for publishing in the library of an area. The Approver can accept a document as it is, request changes where needed or reject the publishing. The Approver is also responsible for the review of the content aimed to appear in the different sections (introduction, events, news etc) before they are published. CIWIN Executives are in charge of appointing national Approvers, as the approving process will remain at national level. It is up to the Member States to decide how many Approvers they need and what is their field of approving competence.

1.7. User

The role of the User is the one with the least power within the CIWIN prototype. A User is a member who is involved in CIP and even though he has access in the CIWIN portal, his rights are limited to viewing/reading content, without being able to modify it.

2. Functionalities

Almost all areas of the CIWIN portal dispose of specific functionalities, to enable the collaboration of CIWIN users and the exchange of information within an area. The basic functionalities foreseen and their description are presented hereunder.

2.1. Discussion forum

Almost all areas have a dedicated discussion forum, facilitating the communication within an area. The access rights attributed to a user will define whether the user is able to participate in a discussion or even whether he has a view on the already existing discussions.

2.2. Information Board

The goal of the Information Board is to announce to the users involved in the area news, updates on past events, and other relevant information related to the area.

2.3. Library

Every area disposes of its own library where the documents relevant to the area are hosted upon approval for publishing by the Approver. In the library space Editors are allowed to create, draft, edit and review their working documents.

All users have access to the library, but based on the user's profile parameters and the document's metadata (such as traffic light info, security levels, sector relevance, Member State ownership, etc) each user will only see the documents available to him/her. What is

more, the user will be able to comment easily on documents without integrating his comments in the document.

2.4. Calendar

Every area disposes of its own calendar where events related to it are added in order to give the possibility to all users of the area to remain updated about interesting events in their area. Events can be posted by Editors and will be published upon approval by the Approver.

2.5. Contact list

This functionality facilitates the search of the contact details of a CIWIN user or of a person related to an area who happens not to be a CIWIN user. A CIWIN user can update his contact details.

In addition to the contact list there is a dedicated contact list with the same functionality specifically for CIP Experts within an area, with the possibility to upload their CV as well as their security clearance.

2.6. Search

Every area disposes of a search functionality for the searching of information within the area. From the homepage, the user can search within the whole portal, but the access rights attributed to a user's role will define the search results that will appear.

3. Fixed Areas

The CIWIN prototype is composed by two categories of areas: the fixed areas and the dynamic areas. The fixed areas are included in the site by default and while their content can be adjusted, the areas themselves cannot be removed or renamed. On the other hand, the dynamic areas do not constitute a permanent part of the site. They will be created on demand and their goal is to serve a specific purpose.

3.1. Member State Area

The purpose of this area is to provide the possibility to every Member State (MS) to have its own area in the CIWIN portal. This particular area aims at putting at the disposal of the Member States a more convenient and organised area for the management of Critical Infrastructure Protection at national level - if the Member State so wishes. For the Member State Area, the option exists that the area is organised in the national language of the Member State to which it belongs. A MS area consists of a library with documents relevant for this MS. It also has a dedicated discussion forum, with the relevant topics for this MS. Each MS also has an information board to announce news and a calendar to announce events. Next to the 27 Member State Areas, there is a 28th Area dedicated to the European Commission.

The use of this area is optional and its implementation depends on the decision of each Member State. Thus, if a Member State does not want such a Member State Area, it will not be possible for users of that Member State to access such area. The organisation, the administration and the content of this area is left exclusively to the Member States through their national CIWIN Executive, who acts as the Manager of this area and has full control over it.

3.2. Sector-Sub-Sector Area

Each sector/sub-sector defined in the CIWIN Project has its own area. So, the CIWIN portal consists of 11 sector areas having a similar structure and a topic specific content dedicated to the specific sector. The Sector Area constitutes also the starting point for the navigation of the user to the sub-sector areas relevant to the sector. There will also be one cross-sectoral area, for topics relevant to all sectors.

A sector/ sub-sector area consists out of a library with documents relevant to this sector/ sub-sector. It also has a dedicated discussion forum per sector/ sub-sector for the topics relevant to this sector/ sub-sector. Each sector/ sub-sector also has an information board to announce news and a calendar for events relevant to the sector/ sub-sector, for the publication of which an approval from the Approver is needed.

3.3. CIWIN Executive Area: for CIP Contact Points

This area is the area for the management of the portal. Access will be granted to the CIWIN Executive of each Member State and to an EU Executive appointed by the Commission in first instance.

This area includes a library, a calendar of events, information board announcing news and a discussion forum facilitating the communication and the exchange of information and best practices between CIWIN Executives. This area serves as the strategic coordination and cooperation platform, to promote and enhance the work and communication as far as Critical Infrastructure Protection is concerned. It is not foreseen to have a dedicated moderator for the forum in this area. It is assumed that the CIWIN Executives will have full control over this area, as they are all on equal basis, and therefore all can do the task of moderation.

3.4. External co-operation area

An external co-operation area addresses the need to guarantee awareness of certain trans-European critical infrastructure information. Access to this area is granted only to EU CIWIN authorised users. The aim of the area is to raise the European awareness about external co-operation in Critical Infrastructure Protection, to encourage the raising of CIP standards outside the EU and potentially provide a basis for an effective co-operation in the event of an emergency.

This area has a library, an information board, a calendar and a dedicated discussion group allowing for discussions within a more controlled setting.

3.5. RAS Area

The objective of this area is to facilitate a rapid exchange of information about potential threats as well as information prior, during and after an event and as a result reinforce the preparedness level in case of the need to respond to an emergency.

Rapid creation of alerts is allowed in this area and a special list with metadata should be filled out before the launching of an alert. One of the metadata requires the selection of addressees. The system also provides for the possibility of additional users to be added.

Each addressee will receive the alert as a task in his to-do-list and he should provide an acknowledgement of receipt. A link will be provided to the related alert area.

The area also hosts a library of open alerts and a library of closed alerts. The possibility is provided to launch alerts for exercise purposes. Access rights are granted only to the recipients of an alert as specified in the metadata.

4. Dynamic Areas

4.1. Expert Working Group area

The goal of this area will be to provide support to the different Expert Working Groups. It will give them the possibility to have their own calendar, information board and dedicated discussion forums, through which the exchange of expertise on specific CIP issues and the communication between them will be facilitated. The area offers an optional authoring functionality providing for a virtual place where a document can be formulated. The document will be started there and whoever from the Working Group wants to contribute to the document, has to do it in this area. Supporting this, a private library can be used till a collaborative document is finalised and published at the main library. In order to enhance even more the collaboration of the Expert Working Groups, if possible, the possibility will be offered to have team meetings, project reports, meeting minutes, project management and user task-lists.

4.2. Project area

Projects related to Critical Infrastructure which are covering different Member States can have their own place in the CIWIN portal. All users involved in the Project are able to consult the latest information concerning the Project, exchange messages and find reports and documents related to the Project through a private library. This area will contribute to an improved communication in relation with the Project.

4.3. RAS area

For each launched alert, the option exists to create a RAS area. This area will be dedicated to information exchange and collaboration directly relevant to this specific alert. It includes a library, an information board for general announcements and a discussion forum.

4.4. Special topics area

This area is dedicated to topics related to Critical Infrastructure which are sensitive and require a higher level of confidentiality. Thus, access to this area is limited to a specified group of people on the need to know basis. This area includes a library, an information board, a calendar and a dedicated discussion forum to highlight events, news, and facilitate discussions within a more controlled setting.

5. CIWIN's Prototype