COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 27.10.2008
COM(2008) 676 final

2008/0200 (CNS)

Proposal for a

COUNCIL DECISION

on a Critical Infrastructure Warning Information Network (CIWIN)

{SEC(2008)2701}
{SEC(2008)2702}

(presented by the Commission)

EXPLANATORY MEMORANDUM

CONTEXT OF THE PROPOSAL

Grounds for and objectives of the proposal

The European Council of June 2004 asked the Commission to prepare an overall strategy to protect critical infrastructure. On 20 October 2004 the Commission adopted a Communication on Critical Infrastructure Protection in the Fight against Terrorism, putting forward suggestions on ways of enhancing European prevention, preparedness and response in the event of 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 in December 2004 endorsed the Commission's plan to propose a European Programme for Critical Infrastructure Protection (EPCIP) and agreed to the Commission setting up a Critical Infrastructure Warning Information Network (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. At the same time, the Commission launched a Communication on the EPCIP. Together, these documents set out the framework for infrastructure protection in the EU. The Communication sets forth the horizontal framework for protecting critical infrastructures in the EU, explaining how EPCIP (including CIWIN) might be put into effect.

The CIWIN initiative is part of EPCIP, being concerned more specifically with the information-sharing process between EU Member States and an information technology system to support that process.

General context

The security and economy of the European Union as well as the well-being of its citizens depend on certain infrastructure and the services they provide. For instance, telecommunication and energy networks, financial services and transport systems, health services, and the provision of safe drinking water and food are all crucial to the EU and its Member States. Any destruction or disruption of infrastructure providing key services, on one hand, and an inappropriate response to this kind of event, on the other, could entail loss of life, loss of property and a collapse of public confidence in the EU. Intricate interdependencies mean that a particular event may have a cascading effect on other sectors and areas of life which are not immediately and obviously interconnected. This kind of interconnectedness has been insufficiently researched, and the result may be insufficient critical infrastructure protection and security for EU citizens.

Critical infrastructure in the European Union is currently subjected to a varying puzzle of protective measures and obligations, with no minimum standards being applied 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. Others are only just starting this process, and might benefit significantly from having access to best practices like risk assessment methodology. 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 duplications of activities resulting from insufficient information on similar situations in other Member States: for example, information on best practice in one Member State might avoid the cost of re-developing a similar practice in others.

Furthermore, there is a fear of exchanging sensitive information among stakeholders. If information is to be exchanged efficiently, an environment of trust and flexibility has to be established.

Existing provisions in the area of the proposal

No provisions on the exchange of information and alerts in the field of critical infrastructure protection currently exist in the EU, although the Commission did, in 2006, propose a Directive on the identification and designation of European Critical Infrastructure (ECI) and the assessment of the need to improve their protection (COM(2006) 787 final). At the same time, the Commission launched a Communication on the EPCIP (COM (2006) 786 final). In June 2008, the Council reached a political agreement on the above mentioned Directive, and its adoption is scheduled for the second half of 2008.

In addition, a number of sectoral Rapid Alert Systems (RAS) exist in the EU. The main difference between CIWIN and the existing RAS is the cross-sectoral nature of CIWIN. None of the existing RAS at this moment provide 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:

– Council Decision establishing a Community civil protection mechanism (recast) (2007/779/EC, Euratom);

– Council Decision on Community arrangements for the early exchange of information in the event of a radiological emergency establishing a Community Urgent Radiological Information (87/600/Euratom);

– Council Directive 82/894/EEC of 21 December 1982 on the notification of animal diseases within the Community (82/894/EEC);

– Council Directive on protective measures against the introduction into the Community of organisms harmful to plants (2000/29/EC);

– Decision of the European Parliament and the Council setting up a network for the epidemiological surveillance and control of communicable diseases in the Community (2119/98/EC);

– Directive of the European Parliament and the Council on general product safety (2001/95/EC);

– Regulation (EC) of the European Parliament and the Council laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (178/2002);

– Commission Decision concerning the development of an integrated computerised veterinary system known as Traces (2003/623/EC);

– Commission Decision amending its internal Rules of Procedure (2006/25/EC, Euratom).

Consistency with the other policies and objectives of the EU

This proposal is fully consistent with the objectives of the EU and specifically with the objective "to maintain and develop the Union as an area of freedom, security and justice, in which the free movement of persons is assured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime".

It is consistent with other policies as it does not aim to replace existing measures, but to complement them with a view to improving ECI protection.

CONSULTATION OF INTERESTED PARTIES AND IMPACT ASSESSMENT

Consultation of interested parties

Consultation methods, main sectors targeted and general profile of respondents

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. 22 Member States provided official responses to the consultation. Around 100 private sector representatives also provided comments. The responses were generally supportive of the idea of creating CIWIN.

– 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 contractor conducted interviews on CIWIN in all of the 27 Member States.

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

Summary of responses and how they have been taken into account

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

The responses to the EPCIP Green Paper and ongoing discussions with all stakeholders have had a major impact in shaping the proposal for CIWIN. Initially, Member States did not have a uniform view on setting up the CIWIN. Some supported it as a multi-level communication/alert system with 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 its forum role; or to an RAS linking the Member States with the Commission. At the time of the consultation, two Member States were against the CIWIN system. As opinions differed, the issue was discussed at regular Critical Infrastructure

Protection Contact Point meetings with Member States. The final concept of CIWIN is the result of these discussions.

Collection and use of expertise

Scientific/expertise domains concerned

Expertise was collected through numerous meetings and seminars held in 2006, 2007 and 2008, as well as through the EPCIP Green Paper consultation process. Information was collected from all relevant stakeholders.

Methodology used

In March 2006, the Commission awarded a contract that included a CIWIN feasibility study, the objective being to collect information on best practices for CIP and to conduct interviews with experts in Member States on the requirements of CIWIN, both as an exchange network and a rapid alert system, taking into account existing infrastructures and networks at national and international levels.

A further aim was to establish a common platform for the exchange of information relevant to CIP.

Main organisations/experts consulted

All EU Member States.

Summary of advice received and used

No mention of the existence of potentially serious risks with irreversible consequences.

Means used to make the expert advice publicly available

Through the Annexes to the Impact Assessment.

Impact assessment

Agreement on the adoption of a separate proposal for CIWIN has been already reached within the EPCIP package, more specifically in the Commission's Communication on the EPCIP. The Impact Assessment envisaged five policy options:

Option 1: No policy option. Under this option no cross-cutting action would be undertaken at European level, and the Member States would be left to address the issue individually.

Option 2: CIWIN as an upgrade of existing RAS. Under this option (which would require both a functional revision of existing IT architecture and modifications to their legal base), CIWIN's role would be to ensure the inter-operability of existing RAS, and making them accessible to different services within the EU and in Member States' ministries. As this would cover a rapid alert function only, any move to add on a platform for the exchange of information and best practices require a significant resource-demanding revision of existing RAS.

Option 3: CIWIN as an open platform for the (unsecured) exchange of CIP related information. This option would require an IT tool that would be open to the general public and would function as a regular internet site. This would certainly help to raise awareness on CIP in Europe and increase direct information exchange among stakeholders. Nevertheless, as the owner of whatever information is uploaded would never know who the final user is, the amount of information uploaded would be severely limited.

Option 4: CIWIN as a secure voluntary multi-level communication/alert system with 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 capable of holding and transmitting sensitive information, classified up to the level of UE RESTREINT. The system would have two main functionalities: (1) a secure forum for the exchange of information, with strong emphasis on 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 to use the entire system, either of the functions, or none at all.

Option 5: CIWIN as a compulsory multi-level communication/alert system with 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, with each Member State being obliged to upload and update the relevant information regularly.

The Commission carried out an impact assessment listed in the Work Programme. Option 4 – CIWIN as a secure voluntary/opt-in multi-level communication/alert system with two distinct functions: a rapid alert system and an electronic forum for the exchange of CIP ideas and best practices — clearly showed the most advantageous ratio between benefits and drawbacks. Under this option, CIWIN would offer a secure environment for the exchange of information, do a lot to build trust among stakeholders, and enable alerts to be exchanged.

A copy of the CIWIN Impact Assessment is attached.

LEGAL ELEMENTS OF THE PROPOSAL

Summary of the proposed action

The aim of the proposed action is to assist Member States to exchange information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risk in support of critical infrastructure protection.

Legal basis

The legal bases for the proposal are Article 308 of the Treaty establishing the European Community and Article 203 of the Treaty establishing the European Atomic Energy Community.

Subsidiarity principle

The subsidiarity principle applies insofar as the proposal does not fall under the exclusive competence of the Community.

The objectives of the proposal cannot be sufficiently achieved by the Member States for the following reason(s).

The subsidiarity principle is satisfied as the measures resulting from 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 to ensure that information is available to all Member States who might benefit from it can certainly be implemented only at EU level.

Community action will better achieve the objectives of the proposal for the following reason(s).

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 coordinating items of information that might already be available but are not shared with others.

Only a European approach can ensure that Member States that wish to share and receive information are treated equally, that co-operation does not geographically discriminate against Member States, and that the information really does reach those who wish to receive it.

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

A growing number of infrastructures are European in scale, which means that a purely national approach is insufficient. There is a clear need to address the broad range of threats that may affect Europe's critical infrastructure.

The proposal therefore complies with the subsidiarity principle.

Proportionality principle

The proposal complies with the proportionality principle for the following reason(s).

This proposal does not go beyond what is necessary in order to achieve the underlying objectives of Member State co-operation in the field, especially with regard to the Member States' willingness to participate. The proposed action allows Member States that do not wish to participate in CIWIN to opt- out of the system.

Compared with the benefits, CIWIN will not have a significant direct financial impact on either Member States' or the EU's budget. As an example, the maintenance costs would be approximately €550 000 per year, while the cost of incidents that CIWIN could potentially prevent or limit are much higher.

Choice of instruments

Proposed instruments: Council Decision.

Other means would not be adequate for the following reason(s):

In order for the CIWIN prototype to become fully functional and available to all EU Member States, a legal basis is needed. As the subject addressed by this legal instrument is specific and not general in scope, a Council Decision is best suited to achieve this goal, and at the same time oblige the users of the system (Member States and the Commission) to respect the potential confidentiality of the information exchanged.

BUDGETARY IMPLICATION

The budgetary impact is estimated in the accompanying financial statement. The programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013 will play a part in implementing this decision.

ADDITIONAL INFORMATION

Simulation, pilot phase and transitional period

There has been or there will be a simulation or a pilot phase for the proposal.

Review/revision/sunset clause

The proposal includes a review clause.

The proposal includes a revision clause.

2008/0200 (CNS)

Proposal for a

COUNCIL DECISION

on a Critical Infrastructure Warning Information Network (CIWIN)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 308 thereof,

Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 203 thereof,

Having regard to the proposal from the Commission[1],

Having regard to the opinion of the European Parliament[2],

Whereas:

(1) 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 Commission's intention to propose a European Programme for Critical Infrastructure Protection and agreed to the Commission setting up CIWIN[3].

(2) In November 2005, the Commission adopted a Green Paper on the European Programme for Critical Infrastructure Protection (EPCIP) which provided policy options on how the Commission could establish EPCIP and CIWIN. The results of the Green Paper consultation confirmed the interest of the majority of Member States in establishing CIWIN.

(3) In December 2006, the Commission adopted a Communication on EPCIP[4] which announced that CIWIN would be set up through a separate Commission proposal and would provide a platform for the secure exchange of best practices.

(4) Several incidents involving critical infrastructure in Europe such as for example the European blackout in 2006 demonstrated the need for a better and more efficient exchange of information in order to prevent or limit the scope of the incident.

---

1 OJ C , , p. .
2 OJ C , , p. .
3 14894/04.
4 COM (2006) 786 final.

(5) It is appropriate to establish an information system that will enable Member States and the Commission to exchange information and alerts in the field of Critical Infrastructure Protection (CIP), to strengthen their CIP dialogue, and contribute towards promoting the integration and better coordination of nationally scattered and fragmented CIP research programmes.

(6) CIWIN should contribute to the improvement of CIP in the EU by providing an information system that could facilitate Member States' cooperation; and offer an efficient and quick alternative to time-consuming methods of searching for information on critical infrastructures in the Community.

(7) CIWIN should, in particular, 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.

(8) CIWIN should avoid duplication and be heedful of the specific characteristics, expertise, arrangements and areas of competence of each of the existing sectoral rapid alert systems (RAS).

(9) The Commission has developed over the years the operational capacity to assist in the response to a wide range of emergencies through several RAS that have a sector specific character, and are directed to specialised services within the EU. Nevertheless, existing RAS do not provide a CIP functionality that would be accessible to a wider range of stakeholders than sectoral authorities or emergency services.

(10) The interdependence of critical infrastructure in Member States and varying levels of CIP in Member States suggest that creating a horizontal and cross-sectoral Community tool for the exchange of information and alerts on CIP would increase the security of citizens.

(11) Taking into account the future availability of the Trans European Services for Telematics between Administrations (S-TESTA) communications network or any alternative secure network operated by the Commission, the Commission should decide on the most appropriate technological platform for CIWIN and require end users to meet the technical requirements established by the Commission.

(12) 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.

(13) Access to the CIWIN should be limited to authorised users in compliance with the established terms, procedures and security measures. While user access in Member States should be limited to competent national authorities, access within the Commission should be limited to competent services.

(14) Any costs arising from the operation of CIWIN at Community level should be met from Community resources and/or from relevant Community programmes.

(15) Any costs arising from the operation of CIWIN at national level should be financed by the Member States themselves, unless Community arrangements provide otherwise.

(16) Since the objectives of the action to be taken, namely secure and rapid information exchange between Member States, cannot be sufficiently achieved by the Member States and can therefore, by reason of the effects of the envisaged action, be better achieved at Community level, the Community may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Decision does not go beyond what is necessary in order to achieve those objectives.

(17) This Decision respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union,

HAS ADOPTED THIS DECISION:

Article 1
Subject-matter

This Decision sets up a secure information, communication and alert system - Critical Infrastructure Warning Information Network (CIWIN) - with the aim of assisting Member States to exchange information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risks related to CIP.

Article 2
Definitions

For the purpose of this Decision, the following definitions shall apply:

“Critical Infrastructure” shall mean those assets, systems or parts thereof located in 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.

"Participating Member State" shall mean the Member State having signed a Memorandum of understanding with the Commission.

"CIWIN Executive" shall mean the CIWIN contact point in relevant Member State or the Commission that ensures adequate use of CIWIN and compliance with the user guidelines within the relevant Member State or the Commission.

"Threat” shall mean any indication, circumstance, or event with the potential to disrupt or destroy critical infrastructure, or any element thereof.

Article 3
Participation

Participation in and use of CIWIN is open to all Member States. The participation to CIWIN shall be conditional upon the signature of a Memorandum of understanding that contains technical and security requirements applicable to CIWIN, and information on the sites to be connected to CIWIN.

Article 4
Functionalities

(1) The CIWIN shall consist of the two following functionalities:

(a) an electronic forum for the CIP related to information exchange;

(b) a rapid alert functionality that shall enable participating Member States and the Commission to post alerts on immediate risks and threats to critical infrastructure.

(2) The electronic forum shall be composed of fixed areas and dynamic areas.

Fixed areas shall be included in the system on a permanent basis. While their content may be adjusted, the areas may not be removed, renamed or new areas added. Annex I contains a list of fixed areas.

Dynamic areas shall be created upon demand, and shall serve a specific purpose. Their existence shall be terminated upon fulfilment of their initial purpose. Annex II contains a list of dynamic areas to be created upon the establishment of the CIWIN.

Article 5
Role of the Member States

(1) Participating Member States shall designate a CIWIN Executive and notify the Commission thereof. CIWIN Executive shall be responsible for granting or denying access rights to the CIWIN within the relevant Member State.

(2) Participating Member States shall provide access to the CIWIN in compliance with the guidelines adopted by the Commission.

(3) Participating Member States shall provide and regularly update relevant CIP information of common EU interest.

Article 6
Role of the Commission

(1) The Commission shall be responsible for:

(a) the technical development and management of the CIWIN, including the IT structure thereof and the elements for information exchange;

(b) laying down guidelines on the terms of use of the system, including confidentiality, transmission, storage, filing and deletion of information. The Commission shall also establish the terms and procedures for granting full or selective access to the CIWIN.

(2) The Commission shall appoint the CIWIN Executive, responsible for granting or denying access rights to the CIWIN within the Commission.

(3) The Commission shall provide and regularly update relevant CIP information of common EU interest.

Article 7
Security

(1) The CIWIN shall be established as a secure classified system, and shall be capable of handling information up to the level of RESTREINT UE.

The Commission shall decide on the most appropriate technological platform for CIWIN and users shall meet the technical requirements established by the Commission.

The security classification of the CIWIN shall be upgraded as appropriate.

(2) Users' rights to access documents shall be on a “need to know” basis and must at all times respect the author’s specific instructions on the protection and distribution of a document.

(3) Member States and the Commission shall take the necessary security measures:

(a) to prevent any unauthorised person from having access to the CIWIN;

(b) to guarantee that, when using the CIWIN, authorised persons have access only to data which are within their sphere of competence;

(c) to prevent information on the system from being read, copied, modified or erased by unauthorised persons.

(4) The uploading of information onto the CIWIN shall not affect the ownership of the information concerned. Authorised users shall remain solely responsible for the information they provide and shall ensure that its contents are fully compliant with existing Community and national law.

Article 8
User guidelines

The Commission shall develop and regularly update User guidelines containing full details of CIWIN's functionalities and roles.

Article 9
Costs

The costs incurred in connection with the operation, maintenance and central functioning of the CIWIN shall be borne by the Community budget. Costs related to users' access to CIWIN within participating Member States shall be borne by participating Member States.

Article 10
Reviewing

The Commission shall review and evaluate the operation of the CIWIN every three years, and shall submit regular reports to the Member States.

The first report, which shall be submitted within three years after the entry into force of this Decision, shall, in particular, identify those elements of the Community network which should be improved or adapted. It shall also include any proposal that the Commission considers necessary for the amendment or adaptation of this Decision.

Article 11
Date of application

This Decision shall apply as from 1 January 2009.

Article 12
Addressees

This Decision is addressed to the Member States.

Done at Brussels,

For the Council
The President

ANNEX I

CIWIN FIXED AREAS

The Fixed Areas referred to in Article 4 shall be comprised of the following:

(1) Member State Areas, offering each participating Member State the possibility to create its own area in the CIWIN portal. The organisation, administration and the content of this area will be the sole responsibility of Member States. The area will be accessible exclusively to users from the respective Member State.

(2) Sector Areas, with 11 separate sectors: Chemical Industry; Energy; Financial; Food; Health; ICT; Nuclear fuel-cycle industry; Research facilities, Space, Transport; and Water. There will also be a cross-sector sub-area for generic topics and issues of relevance to multiple sectors.

(3) CIWIN Executive Area, serving as a strategic coordination and cooperation platform designed to promote and enhance the work and communication as far as Critical Infrastructure Protection is concerned. This area will be accessible to CIWIN Executives exclusively.

(4) EU External Co-operation Area, focusing on raising awareness of external co-operation in Critical Infrastructure Protection and of Critical Infrastructure Protection standards outside the EU.

(5) Contact Directory, to facilitate the search for contact details of other CIWIN users or Critical Infrastructure Protection experts.

ANNEX II

CIWIN DYNAMIC AREAS

The dynamic areas referred to in Article 4 shall be the following:

(1) Expert Working Group Area, to provide support to the work of CIP Expert groups;

(2) Project Area, containing information on projects financed by the Commission;

(3) Alert Areas, which may be created in the event of an alert being triggered in the RAS, and will constitute the channel of communication during CIP-related activities;

(4) Special Topics Area, to focus on specific topics.

LEGISLATIVE FINANCIAL STATEMENT

1. NAME OF THE PROPOSAL:

Council Decision on a Critical Infrastructure Warning Information Network (CIWIN)

2. ABM / ABB FRAMEWORK

Activity 18.05: Security and Safeguarding liberties

Objective 2: Critical Infrastructure Protection

3. BUDGET LINES

3.1. Budget lines (operational lines and related technical and administrative assistance lines (ex- B..A lines)) including headings:

Budgetary line: 18.050800

Heading: Prevention, Preparedness and Consequence Management of Terrorism

3.2. Duration of the action and of the financial impact:

From 2009 onwards

3.3. Budgetary characteristics:

Budget line	Type of expenditure		New	EFTA contribution	Contributions from applicant countries	Heading in financial perspective
18.050800	Non-comp	Diff[5]	NO	NO	NO	3A

[5] Differentiated appropriations

4. SUMMARY OF RESOURCES

4.1. Financial Resources

4.1.1. Summary of commitment appropriations (CA) and payment appropriations (PA)

EUR million (to 3 decimal places)

Expenditure type	Section no.		2009	2010	2011	2012	2013	Total
Operational expenditure[6]								
Commitment Appropriations (CA)	8.1.	a	0,95	0,55	0,55	0,55	0,55	3,15
Payment Appropriations (PA)		b	0,95	0,55	0,55	0,55	0,55	3,15
Administrative expenditure within reference amount[7]								
Technical & administrative assistance (NDA)	8.2.4.	c	NA	NA	NA	NA	NA	NA
TOTAL REFERENCE AMOUNT								
Commitment Appropriations		a+c	0,95	0,55	0,55	0,55	0,55	3,15
Payment Appropriations		b+c	0,95	0,55	0,55	0,55	0,55	3,15
Administrative expenditure not included in reference amount[8]								
Human resources and associated expenditure (NDA)	8.2.5.	d	0,117	0,117	0,117	0,117	0,117	0,585
Administrative costs, other than human resources and associated costs, not included in reference amount (NDA)	8.2.6.	e	0,015	0,015	0,015	0,015	0,015	0,075
TOTAL CA including cost of Human Resources		a+c +d +e	1,082	0,682	0,682	0,682	3,81	
TOTAL PA including cost of Human Resources		b+c +d +e	1,082	0,682	0,682	0,682	3,81	

6 Expenditure that does not fall under Chapter xx 01 of the Title xx concerned.

7 Expenditure within article xx 01 04 of Title xx.

8 Expenditure within chapter xx 01 other than articles xx 01 04 or xx 01 05.

4.1.2. Compatibility with Financial Programming

☒ Proposal is compatible with existing financial programming.

☐ Proposal will entail reprogramming of the relevant heading in the financial perspective.

☐ Proposal may require application of the provisions of the Interinstitutional Agreement[9] (i.e. flexibility instrument or revision of the financial perspective).

4.1.3. Financial impact on Revenue

☒ Proposal has no financial implications on revenue

☐ Proposal has financial impact — the effect on revenue is as follows:

4.2. Human Resources FTE (including officials, temporary and external staff) — see detail under point 8.2.1.

Annual requirements	2009	2010	2011	2012	2013
Total number of human resources	1	1	1	1	1

5. CHARACTERISTICS AND OBJECTIVES

5.1. Need to be met in the short or long term

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, and enable member States to use the rapid alert system concerning CIP.

5.2. Value-added of Community involvement and coherence of the proposal with other financial instruments and possible synergy

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.

[9] See points 19 and 24 of the Interinstitutional agreement.

5.3. Objectives, expected results and related indicators of the proposal in the context of the ABM framework

"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, the operational (sub)objective that CIWIN intends to achieve can be identified as follows:

- to provide an IT tool that will facilitate CIP co-operation between Member States, that will offer an efficient and quick alternative to often time-consuming methods of searching for information, and that will offer Member States the possibility to communicate directly and upload information that they deem relevant.

5.4. Method of Implementation (indicative)

☒ ***Centralised Management***

☒ directly by the Commission

☐ indirectly by delegation to:

☐ executive Agencies

☐ bodies set up by the Communities as referred to in art. 185 of the Financial Regulation

☐ national public-sector bodies/bodies with public-service mission

☐ ***Shared or decentralised management***

☐ with Member states

☐ with Third countries

☐ ***Joint management with international organisations (please specify)***

Relevant comments:

6. MONITORING AND EVALUATION

6.1. Monitoring system

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)?

6.2. Evaluation

6.2.1. Ex-ante evaluation

After the conclusion of the testing period (CIWIN pilot project) in 2009, the Commission will 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 ones).

Furthermore, an Impact Assessment has been carried out, and is attached to this proposal.

6.2.2. Measures taken following an intermediate/ex-post evaluation (lessons learned from similar experiences in the pas

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

– 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 Contact Points meetings.

6.2.3. Terms and frequency of future evaluation

CIWIN shall be assessed against the indicators listed under heading 6.1. after the first 3 years of its establishment.

7. ANTI-FRAUD MEASURES

The protection of the Community's financial interests and the fight against fraud and irregularities form an integral part of this Decision.

Administrative monitoring of contracts and payments will be the responsibility of the relevant Commission service. Each of the operations financed under this decision will be supervised at all stages in the project cycle by the relevant Commission services. Supervision will take

account of contractual obligations as well as of the principles of cost/benefit analysis and sound financial management.

Moreover, any agreement or contract concluded pursuant to this Decision shall expressly provide for monitoring of spending authorised under the projects/programmes and the proper implementation of activities as well as financial control by the Commission, including the European Anti-Fraud Office (OLAF), and audits by the Court of Auditors, if necessary on the spot. They shall authorise the Commission (OLAF) to carry out on-the-spot checks and inspections in accordance with Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and irregularities.

Particular attention will be paid to the nature of expenditure (eligibility of expenditure), to respect for budgets (actual expenditure) and to verify supporting information and relevant documentation (evidence of expenditure).

8. DETAILS OF RESOURCES

8.1. Objectives of the proposal in terms of their financial cost

Commitment appropriations in EUR million (to 3 decimal places)

(Headings of Objectives, actions and outputs should be provided)	Type of output	Av. cost	2009		2010		2011		2012		2013		TOTAL	
			No. outputs	Total cost	No. outputs	Total cost	No. outputs	Total cost	No. outputs	Total cost	No. outputs	Total cost	No. outputs	Total cost
OPERATIONAL OBJECTIVE No.1 [10] **To provide an IT tool that will facilitate CIP co-operation between Member States**														
Action: Create and manage a CIP RAS, and Create a forum for the exchange of best practices														
- Output 1	Hosting of RAS functionality of CIWIN system (secure environment)	0,3	1	0,3	1	0,3	1	0,3	1	0,3	1	0,3	5	1,5
- Output 2	Support and maintenance of the system	0,25	1	0,25	1	0,25	1	0,25	1	0,25	1	0,25	5	1,25

[10] As described under Section 5.3

(Headings of Objectives, actions and outputs should be provided)	Type of output	Av. cost	2009		2010		2011		2012		2013		TOTAL	
			No. outputs	Total cost	No. outputs	Total cost	No. outputs	Total cost	No. outputs	Total cost	No. outputs	Total cost	No. outputs	Total cost
- Output 3	necessary technical support to security accreditation, maintenance, the provision of a helpdesk and training	0,07	1	0,4									1	0,4
TOTAL COST 1		0, 617	1	0,95	1	0,55	1	0,55	1	0,55	1	0,55	5	3,15

8.2. Administrative Expenditure

8.2.1. Number and type of human resources

Types of post		Staff to be assigned to management of the action using existing and/or additional resources (**number of posts/FTEs**)									
		2009		2010		2011		2012		2013	
(18)	(20) AD	(21)	0,5	(22)	0,5	(23)	0,5	(24)	0,5	(25)	0,5
(19) Official or temporary staff[11] (XX 01 01)	AST	0,5		0,5		0,5		0,5		0,5	
Staff financed[12] by art. XX 01 02											
Other staff[13] financed by art. XX 01 04/05											
TOTAL		1		1		1		1		1	

8.2.2. Description of tasks deriving from the action

The main task of Commission officials will focus on the task of the CIWIN Administrator. Therefore, Commission officials will be responsible for the configuration of the solution; will manage the requests for the creation of dynamic areas and will be in charge of creating the dynamic areas and removing unused or abandoned areas. The role of the Administrator will be dedicated to the Commission

8.2.3. Sources of human resources (statutory)

☒ Posts currently allocated to the management of the programme to be replaced or extended

☐ Posts pre-allocated within the APS/PDB exercise for year n

☐ Posts to be requested in the next APS/PDB procedure

☐ Posts to be redeployed using existing resources within the managing service (internal redeployment)

☐ Posts required for year n although not foreseen in the APS/PDB exercise of the year in question

---

11 Cost of which is NOT covered by the reference amount

12 Cost of which is NOT covered by the reference amount

13 Cost of which is included within the reference amount

8.2.4. Other Administrative expenditure included in reference amount (XX 01 04/05 — Expenditure on administrative management)

EUR million (to 3 decimal places)

Budget line (number and heading)	2009	2010	2011	2012	2013	TOTAL
1 Technical and administrative assistance (including related staff costs)						
Executive agencies[14]	NA	NA	NA	NA	NA	NA
Other technical and administrative assistance	NA	NA	NA	NA	NA	NA
- *intra muros*						
- *extra muros*						
Total Technical and administrative assistance	NA	NA	NA	NA	NA	NA

8.2.5. Financial cost of human resources and associated costs not included in the reference amount

EUR million (to 3 decimal places)

Type of human resources	2009	2010	2011	2012	2013
Officials and temporary staff (XX 01 01)	0, 117	0, 117	0,117	0,117	0,117
Staff financed by Art XX 01 02 (auxiliary, END, contract staff, etc.) (specify budget line)					
Total cost of Human Resources and associated costs (NOT in reference amount)	0,117	0,117	0,117	0,117	0,117

Calculation– ***Officials and Temporary agents***

See Point 8.2.1.

[14] Reference should be made to the specific legislative financial statement for the Executive Agency(ies) concerned.

Calculation– ***Staff financed under art. XX 01 02***

NA

	2009	2010	2011	2012	2013	TOTAL
XX 01 02 11 01 — Missions	0,01	0,01	0,01	0,01	0,01	0,05
XX 01 02 11 02 — Meetings & Conferences	0,005	0,005	0,005	0,005	0,005	0,025
XX 01 02 11 03 — Committees[15]	NA	NA	NA	NA	NA	NA
XX 01 02 11 04 — Studies & consultations	NA	NA	NA	NA	NA	NA
XX 01 02 11 05 — Information systems	NA	NA	NA	NA	NA	NA
2 Total Other Management Expenditure (XX 01 02 11)	NA	NA	NA	NA	NA	NA
3 Other expenditure of an administrative nature (specify including reference to budget line)	NA	NA	NA	NA	NA	NA
Total Administrative expenditure, other than human resources and associated costs (NOT included in reference amount)	0,015	0,015	0,015	0,015	0,015	0,075

Calculation - ***Other administrative expenditure <u>not</u> included in reference amount***

NA

[15] Specify the type of committee and the group to which it belongs.