ANNEX

ANNUAL WORK PROGRAMME 2009

PREVENTION, PREPAREDNESS AND CONSEQUENCE MANAGEMENT OF TERRORISM AND OTHER SECURITY RELATED RISKS

INTRODUCTION

This is the third Annual Work Programme adopted under the Council Decision No 2007/124/EC, Euratom, establishing the Specific Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related Risks for the Period 2007-2013" (hereafter: the Programme)\(^1\) as part of the General Programme on "Security and Safeguarding Liberties".

This Programme offers a comprehensive framework and contributes to the development of the European Programme for Critical Infrastructure Protection (EPCIP)\(^2\), as well as policy measures aiming at upholding, and/or guaranteeing security and public order during a crisis situation.

The financial support should achieve general and specific objectives aimed at two main areas:

a) Prevention and Preparedness refers to measures aimed at preventing and/or reducing risks linked to terrorism and other security related risks.

b) Consequence Management refers to the coordination of measures taken in order to react to and to reduce the impact of the effects of a security related incident, in particular resulting from terrorist attacks in order to ensure a smooth coordination of crisis management and security actions.

Actions funded under this Programme have to be based on an all-hazards approach, while countering threats from terrorism as a priority.

The specific objectives of the Programme are the following:

- Within the general objectives, and unless covered by other financial instruments, the Programme shall stimulate, promote and develop measures on prevention, preparedness and consequence management based, *inter alia*, on comprehensive threat and risk assessments, subject to the supervision by the Member States and with due regard to existing Community competence in that matter, and aiming to preventing or reducing risks linked with terrorism and other security related risks.

- With regard to prevention and preparedness of risks linked with terrorism and other security related risks the Programme aims at protecting people and critical infrastructure, in particular by:

  (a) stimulating, promoting, and supporting risk assessments on critical infrastructure, in order to upgrade security;
(b) stimulating, promoting, and supporting the development of methodologies for the protection of critical infrastructure, in particular risk assessment methodologies;

(c) promoting and supporting shared operational measures to improve security in cross-border supply chains, provided that the rules of competition within the internal market are not distorted;

(d) promoting and supporting the development of security standards, and an exchange of know-how and experience on protection of people and critical infrastructure;

(e) promoting and supporting Community wide coordination and cooperation on protection of critical infrastructure.

With regard to consequence management the Programme aims at:

(a) stimulating, promoting and supporting exchange of know-how and experience, in order to establish best practices with the view to coordinate the response measures and to achieve cooperation between various actors of crisis management and security actions;

(b) promoting joint exercises and practical scenarios including security and safety components, in order to enhance coordination and cooperation between relevant actors at the European level.

Risk and threat assessments of specific infrastructures is an area of activity for the Member States or Commission, having due regard to existing Community competences, and may only be undertaken under the leadership of a public authority. However, the development of common methodologies and approaches to risk and threat assessments, which could be shared with others across the European Union, can be proposed by various stakeholders having experience in this field. Such methodologies would be of a generic nature and would not address any specific security issues, but could be used by the interested parties (Member States, infrastructure owners/operators) for such purposes.

This Programme does not apply to matters covered by other financial instruments, in particular by the Rapid Response and Preparedness Instrument for Major Emergencies (now renamed Civil Protection Financial Instrument) and by the research activities in the areas of Security and Space in the 7th RTD Framework Programme.

1. **BUDGET**

<table>
<thead>
<tr>
<th>Part</th>
<th>Types of actions</th>
<th>The budget envisaged</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Calls for proposals for transnational and national projects</td>
<td>€ 14.2 million</td>
</tr>
<tr>
<td>B</td>
<td>Grants to standardisation bodies</td>
<td>€ 0.4 million</td>
</tr>
<tr>
<td>C</td>
<td>Grants to bodies in monopoly situations</td>
<td>N/A</td>
</tr>
<tr>
<td>D</td>
<td>Public procurement</td>
<td>€ 0.7 million</td>
</tr>
<tr>
<td>E</td>
<td>Administrative arrangements with the JRC</td>
<td>€ 2.4 million</td>
</tr>
</tbody>
</table>
*The total amount will be increased as a result of a foreseen participation of EFTA countries. The detailed amount is a subject to further confirmation.

It is envisaged that calls for proposals will be published on the European Commission's website around October 2008.

2. **EXPECTED OUTCOME**

The projects and other actions are expected to contribute to the achievement of the general as well of the specific objectives of the programme. The projects are moreover intended to contribute:

- To the development of instruments (at EU level), strategies and activities/measures in the field of the effective protection of critical infrastructure (at both EU and MS levels) and/or;
- To the development of a common framework for the effective protection of critical infrastructure at EU level.

In addition, the projects should achieve the following results:

- development of methods, techniques and instruments for operational and training use in this particular field;
- exchange and dissemination of information, experience and best practices between Member States and applicant countries and between the different organizations or bodies responsible for the protection of critical infrastructures;
- development and improvement of the relationship between public authorities and private sector in the field covered by the Programme;
- improvement of mutual knowledge of the Member States' protection systems;
- enhancement of the capacity to share good practices;
- creation of informal contact networks between authorities;
- development of a culture of trust and cooperation.

### A. **ACTION GRANTS TO BE AWARDED THROUGH A CALL FOR PROPOSAL (TRANSNATIONAL AND NATIONAL PROJECTS)**

The 2009 budget will fund the following actions with a budget of € 14.200.000. Following a call for proposals, action grants may be awarded to transnational and/or national projects.

All areas identified in the programme “Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks” are open for proposals. However, in 2009, the following priorities have been identified. Proposals submitted outside these priorities will be funded if the available budget permits.

---

3 OJ L58 of 24.2.2007, p.1
(1) Development/evaluation/propagation of tools and methods to design public spaces to improve protection against terrorist attacks, including mitigation of blast effects (structures and injuries) e.g. materials and methods of construction and stand-off protection from improvised explosive devices (person borne and vehicle borne no warning attacks) e.g. long range sensors and physical barriers.

(2) Development/evaluation/propagation of remote and direct assessment techniques to identify individuals who pose security risk e.g. screening for behavioural indicators (relevant to insider threat) linked to detection of hostile reconnaissance, behavioural analysis and intelligent vision systems.

(3) Development, implementation and evaluation of a large-scale pan-European exercise to test Internet contingency plans. The exercise will examine the preparedness and incident response capability to respond to a simulated coordinated attack altering the correct functioning of the Internet resources of Member States and their constituencies. The exercise should fully involve relevant Member States entities as well as relevant European industry for electronic communication networks and services. It should help identify interdependencies as well as gaps in terms of processes, procedures, organisation and protective measures in place.

(4) Development of national business cases for the implementation of priority communications capability on public networks to ensure that critical users can make vital communications on public networks in case of crisis. The study will analyse the rationale, in terms of economic and social costs and benefits, for Member States to plan and support the implementation of priority communications capabilities on public networks. The analysis should firstly take stocks of the current state of Member States' implementation of priority communications capabilities aiming to ensure that critical users can make vital communications on public networks in case of crisis.

(5) Study on public-private partnership initiatives to enhance security and resilience of fixed and mobile telecommunications as well as the Internet. This study will take stock of initiatives and procedures in place in Member States in terms of public-private partnership initiatives to enhance security and resilience of fixed, mobile telecommunications and Internet. The study will set-up a mechanism to foster the exchange of know-how and experience between Member States with regards to public-private initiatives to enhance security and resilience of fixed and mobile telecommunications as well as the Internet.

(6) Development of an effective communication methodology of counter terrorism messages to members of the public in crowded public places e.g. reassurance, vigilance and deterrence.

(7) Development of Inter-dependency modelling tools for the Information Communication Technology sector.

(8) Development/evaluation/propagation of model architectures for robust process control systems which restrict data traffic in critical infrastructures that use process control technology.

(9) Development/evaluation/propagation of real time malicious code identification and network forensic tools.

(10) Development and evaluation of joint exercises and live/practical scenarios aiming at the training and improvement of the coordination of the European Union actors who are involved in the management of terrorist attacks consequences, as well as the
propagation of the acquired know-how through the elaboration of “Best Practices Manuals” to all Member States.

(11) Development/evaluation/dissemination of techniques oriented to protect the assets which form the European electrical grid (high voltage AC transmission towers and transformation substations) against terrorist attacks that could pose a threat to the stability of the system; and the development of large-scale across-Europe exercises to simulate a coordinated attack against the mentioned assets that might alter the correct functioning of the electric grid.

(12) Providing technical expertise and participation of experts in assessments or other mechanisms, including training provided to national or operator experts to support MS in the identification, designation and protection of critical infrastructure both at national and EU levels in the European Union. This action will provide support to the critical infrastructure protection implementation process in the Member States. Detailed and realistic case-studies will be used to validate the methods, in collaboration with experts from the Member States. Technical expertise and training will take into account the common EU guideline on definition and application of method and techniques for ex-ante assessment of infrastructure. This guideline will also enable an approach to determine interdependencies and assessment of cascading effects.

B. GRANTS TO STANDARDISATION BODIES

The total budget envisaged for action grants awarded without a call for proposals is € 400,000 and it concerns CEN, the European Committee for Standardization, recognized as a European standardisation body.

Support to the European Committee for Standardisation (CEN) concerning standardisation activities in the critical infrastructure protection field

CEN, the European Committee for Standardization, was founded in 1961 by the national standards bodies in the European Economic Community and EFTA countries. CEN contributes to the objectives of the European Union and European Economic Area with voluntary technical standards which promote free trade, the safety of workers and consumers, interoperability of networks, environmental protection, exploitation of research and development programmes, and public procurement.

Within the Technical Board Working Group 161 (CEN/BT WG 161), setup following the terrorism attack in New York in September 2001, standardisation activities are undertaken in the field of the security of the citizen. The work of the group concentrates on prevention, preparedness and consequence management issues.

With the objective of supporting CEN in the development of standards related to prevention, preparedness and consequence management, and in particular critical infrastructure protection, grants of a total sum of € 400,000 are foreseen for standardisation activities.

These activities will include:

(1) Standardisation needs on interconnection and interoperability, i.e. the interconnection of networks, access to networks and interoperability of services from an ICT and electricity distribution perspective
(2) Development of security standards specific to industrial control systems (SCADA). Application fields are: energy (electricity, oil, gas), process industries, pharmaceuticals, manufacturing, etc.

(3) Further elaboration and extension of the initiatives on a management system standard with requirements necessary to control risks associated with the handling or storage and disposal of biological agents and toxins in laboratories and facilities, and the auditing and certification activities related to it into European Standards. This action will be harmonized and, where possible, integrated with the related activities in the field of requirements to the competence of a BioSafety Professional (BSP) standard.

(4) Robustness assessment and progressive collapse avoidance provisions in standards for buildings subjected to explosion loads and performance-based criteria in standards for glass panels subjected to blast loads.

C. GRANTS TO BODIES IN MONOPOLY SITUATIONS

None in 2009.

CONDITIONS AND MODALITIES (for all grants)

In line with the Financial Regulation and the basic act, the following conditions and modalities will apply.

1. Financial provisions

   a) The maximum rate of co-financing by the Commission is 70% of the total eligible costs of the project.

   b) Commission grants are given for non-commercial purposes only and projects must be strictly non-profit making.

   c) Grants awarded by this Programme shall be covered by a written agreement, including the modalities for the reimbursement of a specified proportion of the eligible costs actually incurred;

   d) As a general rule, the co-funding is provided in two instalments: a pre-financing payment on signature of the grant agreement, and the balance on receipt and approval by the Commission of the final report and final financial statement.

2. Eligibility

To be eligible, grant applications must meet the following criteria:

   a) Projects must be submitted by bodies and organisations established in the Member States with legal personality. Applications from natural persons are not eligible.

Bodies and organisations which are profit oriented may submit projects only in conjunction with non-profit oriented or state organisations and the project susceptible to be awarded a grant must present a non-profit budget.
b) Projects must match one or more objectives of the programme;

c) Transnational projects must involve partners in at least two Member States, or one Member State and one other State which is an acceding or a candidate country. Third countries and international organisations may participate as partners, but are not permitted to submit projects;

d) National projects are eligible as starter and/or complementary measures to transnational projects, or if they contribute to developing innovative methods and/or technologies with a potential for transferability to actions at Union level, or develop such methods and technologies with a view to transferring them to other Member States and/or candidate countries.

e) Project proposals/action grant requests seeking EU co-funding of less than € 50,000 will not be eligible to receive a grant.

f) Projects cannot be already completed and should be scheduled to start not before the signature of the grant agreement. An earlier start of the project may take place only where the applicant can demonstrate the need to start the action before the grant agreement is signed. In such cases, expenditure eligible for financing may not have been incurred prior to the date of submission of the grant application.

g) Projects cannot last more than two years.

3. Exclusion

Candidates shall be excluded from participating in the call for proposals if they are in one or more of the situations listed in Articles 93 and 94 of the Financial Regulation.

4. Selection criteria

In accordance with Article 116(1) of the Financial Regulation and Article 176 of the Implementing Rules, proposals for projects shall be evaluated on the basis of the following selection criteria:

(a) the applicant's operational and professional competencies and qualifications in the specified area required to complete the proposed action or work programme including evidence of relevant professional training and/or experience for the personnel concerned. In the case of government or law enforcement organisations, evidence that the project falls within their statutory area of responsibility may be submitted to establish their operational and technical competence. Proposals should also show evidence of ability to access information or participants in the way proposed.

(b) the applicant's financial capability, i.e. stable and sufficient sources of funding to maintain its activity throughout the period during which the action is being carried out and to participate in its funding, based on the submitted documents (such as the balance sheets showing the annual incomes and expenditures, cash flow, debts and the amount of cash available).

Only proposals which meet the above selection criteria will be examined in detail.

5. Award criteria
Proposals that are eligible and meet the selection criteria will be assessed by the evaluation committee and they will be ranked on the basis of the following award criteria:

**Conformity.** Projects will be assessed on the extent to which they fall within the priority areas identified in Sections A, B and C above and in the relevant EU strategic documents and/or action plans. For each type of project, it should be demonstrated that the objective of the project reflects a clearly identified need for action according to the EU's policy priorities in the field of Prevention, Preparedness and Consequence management of Terrorism and other Security related Risks.

**Quality** of the proposed action regarding its conception, organisation, presentation, methodology, expertise, expected results and strategy for their dissemination. In particular, the ability of the project to attain the desired objective(s) will be assessed.

**Value for money.** Amount requested for financial support and its appropriateness as to expected results.

**Impact** of the expected results on the general objectives of the Programme and on measures taken in the different domains as specified in Articles 4 and 5 of the Council Decision.

**European dimension.** Wide geographic scope of the project, in terms of partners, participants and the target groups, will be favoured. For national complementary projects, this criterion is replaced by the geographical scope of the measure they complement. For other national projects (starter measures and other actions), it is replaced by the potential geographical scope of follow-up measures.

**Economies of scale.** Larger projects, in terms of for example ambition and participants, will be favoured.

### 6. **Timetable**

The following schedule is envisaged:

- Opinion of the Programme Committee on the WP: July 2008
- Decision by the Commission: September 2008
- Publication of Call for proposals: October 2008
- Deadline for submission of proposals: January 2009
- Opinion of the Programme Committee on the award of: April 2009
- Commitments and grant agreements: From April 2009 onwards

### D. PUBLIC PROCUREMENT

1. **Actions envisaged**

The Commission intends to undertake the following actions in 2009 through appropriate procurement procedures:

_a) IT risk profiles for critical infrastructures_ IT threats to critical infrastructure sectors should be examined for Europe in an IT risk overview study (conducting sectoral threat
assessments focusing on IT). The examination should not only include technical aspects but also address personnel and organizational challenges. The resulting IT risk profiles should be both cross-cutting and sectoral. The study would be classified at EU Confidential level and any successful bidder would need to comply with the necessary security clearances.

**Envisaged budget for this action: € 300.000.**

b) Completion of the development and deployment of CIWIIN (Critical Infrastructure Warning and Information Network).

Procurements through tendering or existing framework contracts for the establishment of a secure and robust technical infrastructure, including hardware and software and support for CIWIN, and also the necessary technical support to security accreditation, maintenance, the provision of a helpdesk and training. The implementation of this action is conditioned to the adoption of the decision to create CIWIN.

**Envisaged budget for this action: € 400.000.**

2. **Budget and estimated schedule/timetable**

The total budget envisaged for contracts is € 700.000. The following schedule is envisaged for items a) to c):

- **Publication of procurement procedures**: 4th quarter of 2008
- **Award of Contracts**: 2nd quarter of 2009

E. **ADMINISTRATIVE ARRANGEMENTS WITH THE JRC**

The Commission intends to undertake the following actions in 2009 through Administrative Arrangements with the Joint Research Centre, with a budget of € 2.400.000.

a) **Establish a voluntary EU reference network for critical infrastructure protection**

The objective of the action is to establish a **European Reference Network for Critical Infrastructure Protection**, hereafter referred to as **ERN-CIP**.

The process leading to the establishment of the ERN-CIP is divided into two successive phases: a **preparatory phase** and an **implementation phase**.

The preparatory phase is to be carried out by administrative agreement with the JRC which will determine the price and the conditions of the task to be performed by the JRC for JLS. This agreement will cover all the operational costs of this implementation.

The objective of the **preparatory phase** is to prepare, together with the Member States, a detailed project plan for establishing the ERN-CIP. To that end, the preparatory phase includes the following tasks:

- review and consolidation of the needs and requirements of the Member States and of the Commission with respect to the ERN-CIP;
- identification of priority areas on which the ERN-CIP will first focus its activity once established;
- inventory of existing European laboratories and facilities relevant for the priority areas;
development of procedures and criteria for managing and joining the ERN-CIP;

development of protocols and procedures for designing, budgeting and running security experiments;

identification of security requirements for storing and sharing the information managed by the ERN-CIP;

preparation of a detailed project proposal for establishing the ERN-CIP.

To carry out these tasks in close cooperation with the Member States, the JRC will contribute with core staff to a dedicated task force consisting of Detached National Experts from Member States who may, if suitable, be hosted by the JRC.

The budget for carrying out the preliminary phase amounts to €600.000. This budget will be used to pay the costs associated with the Detached National Experts, the missions of the task force members, and the meetings and workshops organised by the task force. The JRC core staff will not be paid by the action grant. The preparatory phase is expected to be completed by mid 2009.

The remaining budget of this action will be employed in an implementation phase, on the condition that it is justified in the project proposal and approved by the Member States in Council. The budget allocated for the establishment of the network will not be used for justifying or requesting new staff positions in the JRC.

The objectives of the implementation phase are to carry out the project proposal delivered by the preparatory phase and, ultimately, establish the ERN-CIP. This phase will therefore focus on the formal constitution of the network and the management and running of the network. This include the definition of experimental work programmes, the design and execution of individual security experiments as well as the management and co-ordination of mechanisms for the running of tests by EU public and private stakeholders and the management of tools for the co-ordinated secure collection and sharing of test results and data.

The implementation phase is further broken down into two sub-phases; a) Preparation of Implementation and b) Execution of Implementation. The budget for carrying out the sub-phase Preparation of Implementation amounts to €900.000. It is envisaged that the preparatory implementation phase will be coordinated by the JRC and executed together with the Member States. A sub-delegation from DG JLS to JRC will be established to that effect. The JRC will carry out the necessary calls for tenders. Further funding will be required to implement the execution of implementation.

The main tasks to be developed are:

Preparatory Phase

(1) Analyse the experimental security requirements at the EU level, consulting with public and private stakeholders in the Member States, and taking into consideration the sectors and priorities defined in the context of EPCIP;

(2) Review the current EU-wide security-related test, trial and evaluation capabilities and capacities (i.e. establish what sites already exist and are available in the Member States, where, and with what testing qualifications and resources);
Propose a roadmap for the implementation of the reference network and the development of the needed capabilities, and manage its implementation. Propose and manage the schedule setting and review process;

Propose and set-up the management structure for the reference network. There would be an approval process existing along with the schedule setting process. The approval process would be linked to making sure that all interested and relevant parties have access to the site and the possibility of sharing results on a need-to-know basis;

Implementation Phase

Preparation of Implementation

Develop common testing protocols (i.e. for running and documenting the results of experiments) and support the development of certification standards (e.g. detection equipment);

Investigate and develop mechanisms for the running of tests by EU public and private stakeholders, in the strict respect of confidentiality and secrecy requirements.

Execution of Implementation

Design and develop experiments for the testing of critical infrastructure-related commercial detection and protection equipment (e.g. against explosive material), and provide access to experimental security facilities to carry out the experiments;

Design and develop experiments for testing the vulnerability of critical infrastructure systems (e.g. control systems), and provide access to experimental security facilities to carry out the experiments;

Investigate, develop and manage mechanisms and tools for the co-ordinated secure collection and sharing of test results and data. The test facility would operate on a classified basis with all sensitive test results being classified at EU Confidential level or higher;

Develop and manage mechanisms for the running of tests by EU public and private stakeholders, in the strict respect of confidentiality and secrecy requirements. Subsidised tests would be available to Member States authorities while private sector entities would be required to pay a fee to cover testing costs.

Once established, it is foreseen that the Member States will have access to the testing facilities of the ERN-CIP and will be notified of the execution of security experiments. The ERN-CIP, would inform MS about all conducted experiments; it would then be up to interested Member States to contact the experiment originator and ask for access to the results of the experiment. The experiment originator would decide on the need to know and consequently, on whether to share the info with the requesting party but only if the security requirements are met (e.g. security clearance). This principle would also apply to private sector parties using the facility.

The network will operate in full coherence with other security-relevant European research initiatives such as those outlined in, for example, the Action plan for Enhancing the Security of Explosives; in the European Civil Aviation Conference (ECAC); and by the precursors working group, would enhance all Member State’s capacities.

Envisaged budget for this action: € 1.500.000.

b) Study to define the rationale and propose sectoral criteria for the identification of European Critical Infrastructures
The study will define the rationale and propose sector criteria for the identification of European Critical Infrastructure in the sub-sectors of: "Trading, payment clearing and settlement infrastructures and systems for financial instruments" for "Production and storage/processing of chemical substances" and for "Pipelines of dangerous substances". The sector criteria shall be developed through a dialogue with all stakeholders and by taking into account the cross-cutting aspects with other sectors and dependencies.

Envisaged budget for this action: € 250,000.

c) Assistance to Member States for critical infrastructure protection

Common guidelines on methodology including drafting of operator security plan templates are required during the assessment process of infrastructure. Such guidelines are sometimes non-existent, or cannot be applied in a harmonized way to the criteria that have been defined. This will be laid down in a document that provides a guideline and best-practices for use during the assessment process.

- Definition and application of methods and techniques for ex-ante assessment of infrastructures. The production of the guideline and best-practices document is to be reviewed by the MS before their finalization. The guidelines will set an approach to determine interdependencies and assessment of cascading effects, and which should or should not be included. Detailed and realistic case-studies will be developed to validate the methods, in collaboration with experts from the member-states.

To further ensure harmonized applications during the designation process centralized guidance would be provided to the Member States. This guidance will provide support to the implementation process in the Member States.

- To develop together with Member States experts a CIP support mechanism. Such a mechanism would entail a central helpdesk, a network of experts, or active participation of experts in assessments, training provided to national or operator experts, or other mechanisms. The security issues and procedures required for this work will be defined.

Envisaged budget for this action: € 450,000.

d) Technical support and hosting assistance for CIWIN

If the CIWIN system is established, JRC would provide technical support to the establishment of the technical platform and provision for backup secure hosting facilities to ensure business continuity and disaster recovery. JRC is the only secure Commission location for the back-up server, other than DG JLS. The main server is located in DG JLS.

Envisaged budget for this action: € 200,000.

ACCOMPANYING MEASURES

According to Article 7(3) of the basic act, the Commission may finance administrative and technical assistance activities regarding the management of this Programme.

In particular, this may include the operation of a helpdesk and/or call centre providing information and advice on the programme for applicants, beneficiaries and the public, the payment of external experts, activities regarding the exploitation and dissemination of project results, and the organisation of meetings.

The total budget envisaged for contracts and administrative agreements is € 300,000. The relevant budget line is 18 01 04 16.