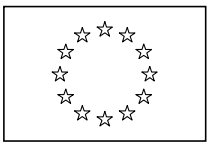

EUROPEAN COMMISSION

Brussels, 12.09.2011
C(2011) 6323 final

COMMISSION DECISION

of XXX

adopting the annual work programme for 2012 for the specific programme on the "Prevention, Preparedness and Consequence Management of Terrorism and other-Security related risks" as part of the General Programme "Security and Safeguarding Liberties"

COMMISSION DECISION

of XXX

adopting the annual work programme for 2012 for the specific programme on the "Prevention, Preparedness and Consequence Management of Terrorism and other-Security related risks" as part of the General Programme "Security and Safeguarding Liberties"

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Council Decision 2007/124/EC, Euratom of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme 'Prevention, Preparedness and Consequence Management of Terrorism and Other Security Related Risks',[1] and in particular Article 8(2) thereof,

Whereas:

(1) In accordance with Article 7 of Decision 2007/124/EC, Euratom, Community support may take the form of grants or public procurement contracts. Community grants shall be awarded further to calls for proposals, save in duly substantiated exceptional cases of urgency or where the characteristics of the beneficiary leave no other choice for a given action, and shall be provided through operating grants and grants for actions.

(2) In accordance with Article 8(2) of Decision 2007/124/EC, Euratom, the Commission shall adopt an annual work programme specifying its specific objectives, thematic priorities, a description of accompanying measures envisaged and if necessary a list of other actions.

(3) The 2012 annual work programme should determine the arrangements for granting financial support to the eligible actions listed in Article 5 of Decision 2007/124/CE, Euratom.

(4) Article 75 of Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities, hereafter referred to as the Financial Regulation,[2] requires that every item of expenditure shall be committed and that the commitment of the expenditure shall be preceded by a financing decision adopted by the institution or the authorities to which powers have been delegated by the institution.

(5) In accordance with Article 110(1) of the Financial Regulation, grants are subject to an annual work programme, published at the start of the financial year.

---

1 OJ L 58, 24.2.2007, p.1.

2 OJ L 248, 16.9.2002, p. 1.

(6) In accordance with Article 90(2) of Commission Regulation (EC, Euratom) No 2342/2002 of 23 December 2002 laying down detailed rules for the implementation of the Financial Regulation, hereafter referred to as the Implementing Rules,[3] the decision adopting an annual work programme within the meaning of Article 110 of the Financial Regulation is considered as the financing decision within the meaning of Article 75 of the Financial Regulation, provided that it constitutes a sufficiently detailed framework.

(7) In accordance with Article 166 of the Implementing Rules, the annual work programme specifies the basic act, the objectives and the schedule of calls for proposals with the indicative amount and the results expected.

(8) The measures provided for in this Decision are in accordance with the opinion of the Committee established by Article 9 of Decision 2007/124/EC, Euratom.

HAS DECIDED AS FOLLOWS:

Article 1

The 2012 annual work programme for the specific programme 'Prevention, Preparedness and Consequence Management of Terrorism and Other Security Related Risks', described in the Annex to this decision, is hereby adopted. This decision serves as a financing decision for 2012 for the budget article 18.05.08 subject to the condition that the budget for 2012 is adopted by the budgetary authority. The total amount covered by this decision is 23.280.000 € subject to the necessary funds being available under the 2012 general budget of the European Union.

Article 2

Cumulated changes to the allocations to the specific actions not exceeding 20% of the maximum contribution authorised by this Decision are not considered to be substantial provided that they do not significantly affect the nature and objective of the work programme. This may include the increase of the maximum contribution authorised by this Decision up to 20%. The authorising officer responsible may adopt such changes in accordance with the principles of sound financial management and of proportionality.

Done at Brussels,

For the European Commission

Member of the European Commission

[3] OJ L 357, 31.12.2002, p. 1.

ANNEX

ANNUAL WORK PROGRAMME 2012

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

INTRODUCTION

This is the sixth 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)[4] 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)[5], as well as policy measures aiming at upholding, and/or guaranteeing security and public order during a crisis situation. It also contributes to the implementation of the Communication "EU Internal Security Strategy in Action" adopted by the Commission on 22 November 2010.[6]

The Commission will ensure complementarity with other European Union initiatives and internal consistency e.g. with the Research and Development Framework Programme 7 security and risk governance themes, as well as other related actions, as in the area of security of energy supply, which includes the protection of energy infrastructures - with due consideration of ethical review and of research on citizenship, fundamental rights and relations between internal and external EU policies. This will be achieved by reinforced inter-service consultation during the implementation phases of the work programme, including with the European External Action Service, given the link between internal and external security, in particular in the area of countering terrorism and protecting critical infrastructure. Any actions funded will be complimentary to the current long term actions in the field of e.g. counter terrorism and protection of critical infrastructure, as financed by the Instrument for Stability.

---

4 OJ L 58, 24.02.2007, p.1

5 Council Directive No. 2008/114/EC:
(a) 'critical infrastructure' means an asset, system or part thereof located in Member States which is 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;
b) 'European critical infrastructure' or 'ECI' means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure;

6 COM/2010/0673 final available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0673:EN:HTML

This annual work programme covers the priorities in 2012 and consists of the following parts and types of actions:

Part	**Types of actions**	**The budget envisaged**
I.	**Grants**	
A	Action grants	18 060 000€
B	Grants to standardisation bodies	N/A
C	Grants to bodies in monopoly situations	N/A
II.	**Public procurement contracts and administrative arrangements**	
D	Public procurement	€ 900 000
E	Actions to be carried out with the JRC	€ 4 320 000
	Total:	**€ 23 280 000**

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

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

- 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 European Union 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:

  - stimulating, promoting, and supporting risk assessments on critical infrastructure, in order to upgrade security;

- stimulating, promoting, and supporting the development of methodologies for the protection of critical infrastructure, in particular risk assessment methodologies;

- 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;

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

- promoting and supporting European Union wide coordination and cooperation on protection of critical infrastructure.

- With regard to consequence management the Programme aims at:

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

  - 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.

Establishing risk and threat assessments of specific critical infrastructures is an area of activity for the Member States or the Commission, having due regard to existing Union 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 the Rapid Response and Preparedness Instrument for Major Emergencies (now renamed Civil Protection Financial Instrument) and the research activities in the areas of Security and Space in the 7th RTD Framework Programme.

It is envisaged that one call for proposals will be published on the European Commission's website in the first quarter 2012.

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 or training use in this particular field;
- exchange and dissemination of information, experience and best practices between Member States and between the different organisations 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

Following a call for proposals, action grants may be awarded to transnational and/or national projects, in accordance with the minimum rate of 65% of the annual expenditure set in the Basis Act[7]. The budget dedicated to calls for proposals is estimated at 18 060 000 €.

All areas identified in the Programme are open for proposals. For 2012, the following priorities have been identified: (proposals submitted outside these priorities will also be considered, subject to quality and budget availability after funding projects matching priorities):

- Facilitating the implementation of Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection;

- Accompanying the development of the policy initiative and the action plan on Critical Information Infrastructure Protection (CIIP) – COM(2009) 149 and COM (2011) 163. In particular, support pan-European exercises on large scale network security incidents; as well as the European participation in international global exercises (building as an initial stage on EU-US cooperation on joint/synchronised trans-continental cyber exercises), further support the cooperation between National/Governmental Computer Emergency Response Teams, in particular with the objective to develop and deploy a European Information Sharing and Alert System, by the end of 2013, and reaching out to citizens and SMEs providing to them tailored information on threats, risks and alerts affecting electronic networks;

[7] Art 7.2 of Council Decision 2007/124/EC, Euratom

- Building on national initiatives, support pan-European cooperation between stakeholders to prevent, detect, and mitigate the spread of malwares;
- Promoting risk analysis and the development of measures to enhance the security and resilience of communication networks and information systems for Smart Grids;
- Security of networked critical energy infrastructures; projects related to existing and future practices in view of technologic developments;
- Security of nuclear critical infrastructures, in particular with respect to the relations between safety and security of such infrastructures;
- Supporting Member States by enhancing communication in order to strengthen cooperation between the public and the private sector (regular meetings to discuss issues of common interest) as well as by improving international cooperation and a cross-border exchange of information between these stakeholders and the relevant institutions at European level;
- Interdependency analysis;
- Compilation of a comprehensive all-hazards catalogue for critical infrastructures;
- Monitoring and assessment of evolving threats with a view to securing critical infrastructures, as well as a common understanding in relation to sectoral, intersectoral and cross-border risk management;
- Models for the convergence of physical and cyber security for industrial critical infrastructure to overcome these traditionally separated security areas;
- Concepts for evacuation systems related to critical infrastructure crisis management, including the evacuation from areas I the neighbourhood of the critical infrastructures;
- Convergent security against cyber-threats; creating systems for forecasting and neutralising cyber-threats, both in the Internet and in interconnected hardware;
- Developing integration tools for stakeholders during critical infrastructure crisis management, taking into account the social causes of the crises;
- Increasing the security awareness of critical infrastructure operators;
- Improving information management with regard to critical infrastructures;
- Increasing critical infrastructure protection capability in the transport, energy, ICT, chemical, financial, water, food, health, space, research and nuclear sectors.

B. GRANTS TO STANDARDISATION BODIES

None in 2012.

C. GRANTS TO BODIES IN MONOPOLY SITUATIONS

None in 2012.

CONDITION 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

- The maximum rate of co-financing by the Commission is 90% of the total eligible costs of the project.

- Projects must be strictly non-profit making following Art. 109 (2) of the Financial Regulation.

- 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;

- As a general rule, the co-funding is provided in two instalments: a pre-financing payment corresponding to 80% of the Commission subvention on signature of the grant agreement (lodging a bank guarantee in advance may be requested from beneficiaries to limit the financial risks connected with the payment of the pre-financing), 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:

- Proposals 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.

- Proposals must match one or more objectives of the programme;

- Transnational projects must involve co-beneficiaries (‘partners’ that will receive funding from the Commission) in at least two Member States, or at least one Member State and a candidate country. Organisations in third countries, EU Agencies and international organisations may participate as associate partners on a non-cost basis (‘partners’ not receiving funding from the Commission), but are not permitted to submit projects;

- National projects are eligible as starter and/or complementary measures to transnational projects, or as a contribution to developing innovative methods and/or technologies with a potential for transferability at Union level, or as a development of such methods and technologies with the view to transfer them to other Member States;

- Proposals seeking EU co-funding of less than € 100.000 will not be eligible to receive a grant.

- Subcontracting of a limited part of the action may be eligible up to 30% of the total eligible costs of the project.

- 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 be accepted 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 the award of the grant.

- 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(1) 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:

- 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.

- 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 match priority areas identified in Section A above and in the relevant EU strategic documents and/or action plans. Projects should demonstrate that their objectives reflect 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), quality of budgeting and project management will be assessed.

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 added value. European added-value includes geographical coverage of a project but, most of all, analysis and experimentation that lead to recommendations for common models, protocols, guidelines, structures, mechanisms, policies and processes. In practice, it

implies that, over and above the attempt to run the project in a number of Member States and build multinational partnerships, applicants must look beyond the confines of the project to find the broader European relevance of the issues, the actions and the output of the project. Every project should include a plan for the implementation of results with a clear indication of how the project can be further developed at EU level, the means to make available project relevant information and conclusions to general public and/or interested third parties, and with a statement of its potential for European debate and action;

Value for money. Amount requested for financial support and its appropriateness as to expected results. Larger projects, in terms of, for example, ambition and participants, will be favoured.

6. Timetable

The following schedule is envisaged:

Inter-services consultation	July 2011
Opinion of the Programme Committee	August 2011
Decision by the Commission	September 2011
Publication of Call for proposals	1Q2012
Deadline for submission of proposals	2Q2012
Opinion of the Programme Committee on the award of grants	4Q2012
Commitments and grant agreements	From 4Q2012 onwards

D. PUBLIC PROCUREMENTS

1. Actions envisaged

The Commission intends to undertake the following actions in 2012 through appropriate procurement procedures:

a) Support for Critical Infrastructure Protection expert groups

This action provides for the organisation and support of Critical Infrastructrure Protection expert meetings as required, including an EU-US expert meeting.

Envisaged budget for this action: € 0.3m

b) Study to support the development of reference scenarios in the preparedness, response to disasters and consequence management within the nuclear sector

The objective of this action is to support the work on the development of reference scenarios for disasters involving nuclear critical infrastructure within the EU. The action will be based

on an all-hazards approach, and will focus primarily on the collection and analysis of available data within the EU and beyond. Based on collected information, possible scenarios of nuclear incidents/accidents will be developed and key assets needed for the response to such disasters identified.

Envisaged budget for this action: € 0.3 m

c) Study on approaches to protection of critical infrastructures in third countries and existing international cooperation arrangements

Study on the approaches taken by different States around the world towards protection of their critical infrastructures, and international cooperation in this area. The study should provide an overview of a specific number of case studies of States around the world, detailing the approaches taken to Critical Infrastructure Protection and identifying best practices, as well as describing the different approaches taken to international cooperation in this area.

Envisaged budget for this action: € 0.3 m

The total budget envisaged for contracts is € 900 000.

E. ACTIONS TO BE CARRIED OUT WITH THE JRC

The budget of € 4.320 000 for these actions will be the subject to administrative arrangements for the provision of services, the supply of products or the execution of works concluded between the Commission and the JRC under Article 116(7) of the Implementing Rules. In cases where these actions imply further re-distribution of the funding to third parties by way of substantial procurement procedures or grants, these actions will be subject of co-delegation or crossed sub-delegation.

1.1. Operational and technological support for pan-European exercises on large-scale network security incidents

The purpose of this activity is to provide operational and technological support for the organization and running of pan-European exercises on large-scale network security incidents involving Member States' authorities and relevant stake holders.

The first pan-European exercise on Critical Information Infrastructure Protection (CIIP), CYBEREurope2010, was organised by EU Member States, facilitated by the European Network and Information Security Agency (ENISA) and supported by the Joint Research Centre.

In addition, the purpose of the activity is also to provide operational and technological support to the development of exercises with third countries, in particular with the United States.

Duration: 18 months

Envisaged budget for this action: € 0.6m

1.2. Vulnerability and Protection of High Precision Timing Services for Critical Infrastructures

A number of critical infrastructures and services are currently relying on GPS for precise timing and synchronization (power grids, financial networks, telecom networks, railways,

etc). It is well recognized (e.g., April 2011 UK Royal Academy of Engineering Report on over-dependence on GPS) that this dependence on GPS timing constitutes a single point of failure for multiple critical infrastructures and services. One threat that has not been addressed sufficiently is that posed by GNSS spoofing and the impact this may have on infrastructures relying on GNSS for precise timing and synchronization. A possible effective counter-measure against this threat is the encryption of a commercial GNSS signal (e.g., as originally planned with Galileo E6). This solution would open a very important market for this new type of service that is not currently available from any other GNSS system (GPS, GLONASS).

Design and implementation of signal authentication and added benefits brought by this solution will be the subject of this action. In addition, we would explore the combined use of GNSS and terrestrial precise timing services such as LORAN, to provide additional resilience to precise timing services.

The protection issue is related to the infrastructure needed to monitor the GNSS bands and identify sources of interference. A possible activity complementary to the previous related work for DG HOME could be that, after having quantified the vulnerabilities of commercial timing GNSS receivers currently in the market, we could investigate the extent of the impact of a spoofing attack on the timing accuracy. This investigation would be instrumental in establishing minimum security requirements for GNSS clocks used in Critical Infrastructrure Protections. It is important to note that at present, the actual extent of the risk posed by GNSS spoofing is largely unknown. Therefore such a study could be of interest to DG HOME and would help establish harmonized recommendations to protect CIs in the EU.

Duration: 24 months

Envisaged budget for this action: € 0.4m

1.3. Protection of space-based infrastructures and services

Space-based infrastructure and services have become essential enablers of Critical Infrastructures, and are beginning to be seen as a critical infrastructure in their own right. These include Earth-observation systems such as GMES, Global Positioning System (GPS), EGNOS, Galileo and a vast range of satellite-based commercial services for broadcasting, communications and data. Due to pervasive reliance on space-based services, it is important to assess threats, both natural and man-made, to the space-based infrastructure and services.

This action will be composed of the following tasks:

(a) Develop an inventory of space-based assets (infrastructure and services) that may be classified as part of a critical infrastructure;

(b) Identify a range of man-made threats and natural hazards to space-based assets;

(c) Systematic assessment of risks to the space-based infrastructures and other Critical Infrastructures dependant on the former;

(d) Specific technical studies on the impact of space weather (as a natural hazard) on Critical Infrastructures;

(e) Develop a methodology for impact assessment of abnormal space weather events on space-based services;

(f) Develop a network of ground-based monitoring stations for the effects of space weather on GNSS, with a special focus on the EU's GNSS systems (Galileo/EGNOS).

Duration: 24 months

Envisaged budget for this action: € 0.5m

1.4. Vulnerabilities and protection of communication systems in Smart Grids

The activity (by JRC STA Unit) aims at investigating vulnerabilities of the telecommunication and internet systems used in the Smart Grids, investigate the impact on the energy infrastructure and identify potential protection techniques.

The proposal will use simulation tools to model the impact of a threat (e.g., cyber security attack, internal failure or natural cause) on the communication system and the related energy infrastructure. Protection techniques, which could channeled to the standardization process, will also be identified and described. For example: network management and high availability solutions for IP networks could be tailored to Smart Grids.

The modeling and simulation activity will be complemented by a test bed with real communication equipment and sensors commonly used in smart grids. The purpose of the test bed is to reproduce threat scenarios with real equipment and compare the outcome with the simulation results.

This proposal is linked to the Smart Grid Simulation Centre proposal by IE. The modeling of the communication systems may contribute directly to the Smart Grid Simulation Centre.

With this study, the JRC can provide advice to the policy makers developing and implementing the current energy security policies.

Duration: 24 months

Envisaged budget for this action: € 0.55m

1.5. Modelling and simulation for risk assessment in integrated cyber-physical systems

This activity builds upon existing JRC expertise on instrumentation and industrial control systems in order to develop the capabilities for an experimental assessment of risk in critical cyber-physical systems due to events related with the ICT instrumentation.

A characteristic example of a critical physical system is the electrical grid which is tightly interconnected with a cyber system i.e. IP based networks for control, monitoring as well as other functions e.g. related to energy market.

The main innovations and the steps forwards are:

a) the ability to analyze the impact of cyber events on physical properties by simulating physical systems e.g. impact on the electricity output (in kW).

b) the progressive shift from a local infrastructure perspective, e.g. a single power plant, to a macroscopic level which fits to a European Critical Infrastructure perspective e.g. the electrical grid or Smart Grid.

c) by integrating in the experimental approach modeling and simulation of human Critical Infrastructure operators, e.g. their situation awareness and their actions.

This activity will focus on the electricity grid and the future Smart Grid but the developed approach will be extensible and applicable to a wide spectrum of cyber-physical systems and networks like those found in the transport sector e.g. in aviation.

Deliverables:

1. Report on the Cyber-Physical experimentation approach

2. A study of the impact of cyber network events to physical systems in a macroscopic level e.g. power grid.

3. What-if analysis by modeling and simulation of human operator decisions

Duration: 24 months

Envisaged budget for this action: € 0.5m

1.6. Analysis of the impact of natural hazards and disasters on oil transport pipelines (Natech risk)

The activity (by JRC STA Unit) will study failures in transport pipelines due to natural hazards and disasters (e.g. lightning, floods, earthquakes etc.) that lead to the release of hazardous materials and to supply-disruption. The purpose of the action is the identification of system weaknesses under natural-event loading, the ensuing failure modes and damage states, as well as the final consequences in terms of their impact on safety and supply security. Recommendations for realistic Natech scenario development and for prevention/mitigation measures will also be formulated.

Duration: 24 months

Envisaged budget for this action: € 0.2M

1.7. Development of methodologies for the analysis of networked systems and complex infrastructures

The proposed research (by JRC STA Unit) intends to face the problem of modelling and analysis of networked systems and complex infrastructures, with a focus on resilience and vulnerabilities.

In particular the activity for 2012 will be focused on the development of a new modelling framework for the analysis of networked systems and infrastructures. In particular:

Modelling critical infrastructures from dependability viewpoint considering complexity aspects, structural properties, logic order, static and dynamic attributes, as well as fault propagation and recovery;

- Resilience analysis of networked systems: an approach based on the control paradigm.

The developed methodology will be implemented in a software prototype. Dependability attributes at node level of a network can be modelled and analysed by means of the methodologies and tools already developed at the JRC.

Duration: 24 months

Envisaged budget for this action: € 0.37M

1.8. Smart Grid Simulation Centre

The JRC Energy Security Unit aims at setting up a Smart Grid Simulation Centre, analysing behaviours and characteristics of the evolving electricity systems.

The Smart Grid Simulation Centre will include and expand ESU offline tools for visualisation and analysis of critical electricity infrastructures already developed for the EC policy-making services (more info in the website of the ESU Smart Electricity Systems Action: http://ses.jrc.ec.europa.eu/). The activity will be coordinated with JRC/IPSC tasks on the ICT aspects of smart grid.

The Smart Grid Simulation Centre will allow customised dynamic analysis and representation of the failure effects on power systems, providing geographical, numerical and graphical information in an interactive environment. The Smart Grid Simulation Centre will develop and validate methods, concepts and processes for the analysis and testing of elements and systems of the future smart electricity grid. The modular real-time simulation and hardware-in-the-loop capabilities will be the main tools for the study of the physical and cyber elements of a European interconnected and integrated power grids with the goal of optimising security of electricity supply.

With this Centre, the JRC will be able to provide thorough and rigorous advice to the policy makers developing and implementing the current energy security policies and the upcoming low carbon 2050 strategy.

Duration: 24 months

Envisaged budget for this action: € 0.5M

1.9. Interdependencies between Natural Gas and Power

The JRC Energy Security Unit aims at analysing the interdependency between the natural gas and power systems at the European level, with the integration of simulators and the application of relevant scenarios. The activity will be carried out in conjunction by the Smart Electricity Systems and Security of Supply Actions.

The purpose of this activity is to assess consequences due to interdependency between natural gas and power systems. Natural gas is already (in addition to household and industry) used for flexible power production. Current plans for an increased installation of renewable energy sources (with an intermittent characteristic) will further increase the role of gas as a back up for electric power production. Strong interconnection makes it likely that a failure in gas network triggers failure in the electricity grid and vice versa.

The proposed study will include:

- identification and characterisation of interdependencies,

- analysis of consequences in each system due to failures in the other,

- development of a strategy for modelling interdependency (based on existing JRC models for gas and power networks) and analysing failures and consequences

- recommendations for MS on the need for risk management of interdependencies.

Duration: 18 months

Envisaged budget for this action: € 0.35M

1.10. Analysis of the Vulnerability of the European Gas Transmission Network

The JRC Energy Security Unit aims at analysing the vulnerability of the overall European gas system, based on the development of appropriate models of the gas flows and infrastructure. This activity will contribute to the application of the Regulation 994/2010 on the Security of Gas Supply, and it will be carried out by the Security of Supply Action.

The purpose of this activity is to expand existing models of the European natural gas system and gas transmission network (developed in the last years for DG ENER) in order to:

- cover additional important regions (currently the model includes 9 EU countries);

- add vulnerability and reliability analysis capabilities, with the simulation of different disruptions (attacks, natural disasters, political actions) and operational conditions (i.e., summer, winter);

- develop strategies and methodologies for the identification and characterisation of the most significant potential threats in order to develop relevant disruption scenarios

- apply disruption scenarios for the identification of weak network points

- define the information needs for each operator, and the data exchange needs among operators, for the planning of risk mitigation and emergency planning actions.

Duration: 18 months

Envisaged budget for this action: € 0.35M

The total budget envisaged for the actions to be carried out with the JRC is € 4.320.000.

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 through public procurement.

In particular, this may include the payment of external experts, activities regarding the exploitation and dissemination of project results, production of information material and the

organisation of meetings. The execution of these activities is subject to the available resources on budget line 18 01 04 16.